CA Identity Manager™

Versionshinweise

12.6.5



CA Technologies-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA Technologies:

- CA CloudMinder™ Identity Management
- CA Directory (NeteAuto-Verzeichnis)
- CA Identity Manager ™
- CA Identity Governance (früher CA GovernanceMinder)
- CA SiteMinder®
- CA Berichte zu Benutzeraktivitäten
- CA AuthMinder ™

Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Inhalt

Kapitel 2: Hinweise zur Installation 37

Kapitel 3: Upgrades 45

Kapitel 4: Behobene Probleme 53

Kapitel 5: Dokumentation 63

Anhang A: Barrierefreiheitsfunktionen 67

Kapitel 6: Bekannte Probleme 75

Kapitel 1: Neue Funktionen

Dieses Kapitel enthält folgende Themen:

12.6.4

Änderungen an vorhandenen Funktionen

CA Identity Manager unterstützt die neue Version von CABI

Ab dieser Version unterstützt CA Identity Manager nur Version 3.3 SP1 von CA Business Intelligence (CABI). Das Installations-Kit fürCA Identity Manager enthält die Installationsprogramme für CABI 3.3 und CABI 3.3 SP1. Sie müssen zunächst CABI 3.3 und danach CABI 3.3 SP1 installieren.

Neue Zertifizierungen

Folgende neue Plattformen sind mit CA Identity Manager r12.6.4 zertifiziert:

Endpunkte

- CA Control Minder r12.8 als Endpunkt
- Windows Server 2012 R2 Active Directory als Endpunkt
- Oracle 12c-Datenbank als Endpunkt
- Microsoft Lync Server 2010 und 2013 als Endpunkt
- PeopleSoft Financials 9.2 als Endpunkt
- System for Cross-domain Identity Management (SCIM) als Endpunkt
- Lotus Notes Domino 9.x als Endpunkt

Webservices (Layer7)-Endpunkte

- Service Now
- Microsoft Azure
- Zendesk

Anwendungsserver

- JBoss 6.2.0 EAP

CA Identity Manager-Benutzerspeicher

- Oracle 12c
- Microsoft Windows 2012 R2 Active Directory

CA Identity Manager-Objektspeicher

- Oracle 12c

Credential Provider

- Microsoft Windows 8
- Microsoft Windows 8.1

Zusätzliche Unterstützung

- Agent-Unterstützung der Kennwortsynchronisierung unter Windows Active Directory 2012 R2
- Integration mit CA SiteMinder r12.52 CR1, r12.52 SP1 und r12.51 CR3
- Browser-Unterstützung für IE 11.x
- Browser-Unterstützung für Firefox 29.x

Verbesserung des Top Secret V2-Connector für die Unterstützung zusätzlicher Objekte/Attribute

Der Top Secret V2-Connector wurde verbessert, um Ressourcen, Einrichtungen, Segmente und sämtliche weitere Attribute im Mainframe darzustellen.

Verbesserungen der Kennwortänderung für die Anwendung für Mobilgeräte

Die Kennwortzurücksetzung in der App für Mobilgeräte erfolgt nun über zusätzliche Sicherheitsebenen, die PIN- und Q&A-Abläufe umfassen. Weitere Informationen finden Sie im *Administrationshandbuch*.

Verbesserungen am Massendatenlader-Client

Der Massendatenlader-Client wurde verbessert, um Kettle Transform auf ähnliche Weise wie die Benutzeroberfläche für Massenaufgaben als Datenquelle und als sekundäre Aktion zu unterstützen.

Unterstützung des Android-Betriebssystems durch die mobile Anwendung

Die mobile Anwendung unterstützt nun Mobilgeräte, die das Android-Betriebssystem verwenden.

Unterstützung der benutzerdefinierten Anpassung des SCIM- und Webservice-Connector durch Connector Xpress

Connector Xpress wurde verbessert, um die benutzerdefinierte Anpassung von Metadaten des SCIM- und Webservice-Connector zu unterstützen

- Service Now
- Azure
- Zendesk

Policy XPress unterstützt SOAP- und REST-Webservices

Policy XPress wurde verbessert, um die Webservices SOAP (mit Standardauthentifizierung) und REST (mit Standardauthentifizierung, Proxy-Authentifizierung und OAuth-Authentifizierung) zu unterstützen, um eine Integration mit externen Anwendungen mit Webservice-Schnittstelle zu ermöglichen.

Suchfenster in der Aufgabe "Meine Arbeitsliste anzeigen"

Zur Aufgabe "Meine Arbeitsliste anzeigen" wurde ein neues Suchfenster hinzugefügt, in dem Sie nach der Benutzer-ID des Workflow-Betreffs oder nach dem Initiator der Aufgabe suchen können, um die Arbeitselemente zu filtern.

12.6.3

Neue Zertifizierungen

Die folgenden neuen Plattformen sind mit CA Identity Manager r12.6.3 zertifiziert:

Endpunkte

- Microsoft AD Exchange Server 2013 als Endpunkt
- Salesforce v24 als Endpunkt
- Solaris 11.1 als Endpunkt
- SUSE 11 SP3 als Endpunkt
- CA Directory r12.0 SP12 GA als Connector Xpress JNDI-Endpunkt
- CA ACF2 LDAP r15.1 als Endpunkt
- CA RACF LDAP r15.1 als Endpunkt
- CA TSS LDAP r15.1 als Endpunkt

Server-Betriebssysteme

- Windows 2012 Essentials

Server-Client-Betriebssysteme

- Windows 2012 Essentials
- Windows 8

Anwendungsserver

- JBoss 6.1.1 EAP

CA Identity Manager-Benutzerspeicher

- CA Directory r12.0 SP12 GA
- Microsoft Active Directory 2012 Essentials
- Microsoft ADAM 2012 Essentials

Zusätzliche Unterstützung

- Agent-Unterstützung der Kennwortsynchronisierung auf Active Directory 2012 Essentials
- Internet Explorer 10.x
- Google Chrome 28.x
- Integration mit CA SiteMinder r12.5 CR3, r12.51 CR1
- Unix Agentless-Unterstützung auf RHEL, SUSE, Solaris, AIX und HPUX
- Unterstützung von Unicast und Multicast mit JBoss 6.1.0 EAP
- Unterstützung von CAM 1.14 mit Remote-Agenten dieser Version

- Unterstützung von AXIS21.6.2 mit dieser Version

Unicast-Support für JBoss 6.1 EAP

Für Kunden, die CA Identity Manager auf JBoss 6.1 EAP installiert haben, ist Unicast ein alternatives Messaging-Protokoll zu Multicast. Wir empfehlen Ihnen, beide Protokolle zu testen, um die beste Wahl für Ihre Organisation zu bestimmen.

Weitere Informationen über das Verwenden beider Protokolle finden Sie im *Upgrade-Handbuch* der JBoss-Version.

Neue Ereignisse generieren E-Mails und Audit-Daten

Sie können E-Mail-Benachrichtigungen und Audit-Daten für zwei neue Ereignisse aktivieren:

- ForgottenPasswordAuditEventQnAInitiated

  Die öffentliche Aufgabe "Kennwort vergessen" generiert dieses Ereignis, wenn ein Benutzer die Seite mit der Frage und der Antwort sieht, während er versucht, ein Kennwort zurückzusetzen.

- ForgottenPasswordAuditEventQnALocked

  Die öffentliche Aufgabe "Kennwort vergessen" generiert dieses Ereignis, wenn die Seite mit der Frage und der Antwort gesperrt wird, da Sicherheitsfragen falsch beantwortet wurden.

Sie konfigurieren E-Mail-Benachrichtigungen und Überwachung über die Management-Konsole.

Hinweis: Weitere Informationen über das Konfigurieren von E-Mail-Benachrichtigungen finden Sie im *Administrationshandbuch*. Weitere Informationen über das Konfigurieren von Überwachung finden Sie im *Konfigurationshandbuch*.

Support von ID-Vault in Lotus Notes Domino

Die ID Vault-Funktion von Lotus Notes Domino wird jetzt für diese Version unterstützt. Mit dieser Funktion können Sie nativ und sicher Kennwörter wiederherstellen und zurücksetzen, verlorene IDs wiederherstellen, Benutzer umbenennen usw.

Erfassung von HTTP-Header-Informationen

Neuer Servlet-Filter: ClientExtractFilter wurde zu dieser Version hinzugefügt. Dieser Servlet-Filter ist ein zentraler Ort, um alle Informationen zu erfassen, die sich auf die Web-Client-Umgebung beziehen. Dieser Filter erfasst Informationen von HTTP-Headern. Derzeit werden nur Client-IP-Adressen erfasst. Wir versichern, dass diese Informationen bei einer Anfrage nur einmal erfasst werden.

Dieser Servlet-Filter wird für jede Anfrage ausgeführt, wie vom URL-Muster:/* in web.xml vorgeschlagen.

Die Hilfsprogrammklasse "WebClientInformation" wurde hinzugefügt, die als Platzhalter für Web-Client-Informationen agieren, die in den Filter extrahiert wurden. Diese Klasse enthält derzeit nur die IP-Adresse. Dies wird möglicherweise zukünftig noch erweitert.

Dann wird "WebClientInformation" in "TaskSession" als Attribut eingefügt, das von einem Schlüssel identifiziert ist: WebClientInfo. So werden alle Ereignisse, Aufgaben, Benutzeroberflächen oder Workflows, die als Ergebnis einer Anfrage erstellt wurden, Client-Informationen haben, wo diese Anfrage generiert wurde.

Verbesserungen des Serviceobjekts

Das neue Kontrollkästchen "Revoke services for users" (Services für Benutzer widerrufen) legt fest, ob der Service vor der Löschung widerrufen werden muss oder nicht zur Aufgabe "Benutzer löschen" hinzugefügt wurde.

Die Unterstützung eines Filters für die Aufgabe "Zugriff anfordern und anzeigen" wurde hinzugefügt, sodass der Benutzer den Suchabschnitt für Admin und Eigentümersuchoptionen erhält.

Spezifische Informationen zur Service-Anfrage, wie z. B. Dauer der Service-Anfrage, Benutzerdaten werden im Workflow-Element der Genehmigung für Service-Anfragen sichtbar. Diese Informationen werden auch in E-Mail-Benachrichtigung gesendet, wenn der Workflow auf einer globalen Richtlinie basiert, der auf dem Ereignis "AddServiceToUserEvent" konfiguriert ist.

12.6.2

Neue Zertifizierungen

Die folgenden neuen Plattformen sind mit CA Identity Manager r12.6.2 zertifiziert:

Endpunkte

- CA ControlMinder r12.6 SP2 als Endpunkt
- CA ControlMinder r12.7 als Endpunkt
- Windows Server 2012 als NT-Endpunkt
- Windows Server 2012 (ADAM) als JNDI-Endpunkt
- CA Directory r12.0 SP11 als JNDI-Endpunkt
- Windows Server 2012 Active Directory als Endpunkt
- Java Mainframe Connector als Endpunkt
- Microsoft AD Exchange Server 2010 SP3 als Endpunkt
- Microsoft Office 365 als Endpunkt
- SAPJCO V.3 als Endpunkt

Anwendungsserver

- JBoss 6.1 EAP
- WebSphere Application Server (WAR) 8.0
- WebSphere Application Server (WAR) 8.5

CA Identity Manager-Benutzerspeicher

- CA Directory r12.0 SP11 GA

CA Identity Manager-Benutzerspeicher und Objektspeicher

- Microsoft SQL Server 2008 R2 SP2
- Microsoft SQL Server 2012 SP1

  Hinweis: JBoss hat keine Unterstützung für Microsoft SQL Server 2012 bekannt gegeben.

Zusätzliche Unterstützung

- Java JDK 1.7.x
- Microsoft SQL Server 2012 SP1 - Benutzerdefinierte Rollen und benutzerdefinierte Server-Rollen
- Mozilla Firefox 18.x
- BusinessObjects Report Server XI 3.1 SP6 (CABI 3.3 SP1)
- Integration mit CA SiteMinder r12.5 CR1, r12.5 CR2, r12.5.1, r12.0 SP3 CR12 und r6 SP6 CR10

- Integration mit CA Identity Manager mit CA Identity Governance r12.5 SP8 und CA Identity Governance r12.6 SP1
- Unterstützung mobiler Apps
- Unterstützung für WorkPoint-Designer, Version 3.4.2.20080602-33
- Unterstützung für Microsoft ADS/Exchange Agentless-Modus, DAG und Automatic Mailbox Distribution
- CA AuthMinder v7.1-Unterstützung

Unterstützung mobiler Apps

Die mobile CA Identity Manager-App befähigt Sie, Ihre bestehende CA Identity Manager-Infrastruktur so einzusetzen, dass Benutzer die folgenden Aufgaben über ein mobiles Gerät wie einem iPhone oder iPad ausführen können:

- Zurücksetzen von vergessenen Kennwörtern

  Hinweis: Wenn Sie mobilen Benutzern ermöglichen, ein vergessenes Kennwort über deren Gerät zurückzusetzen, verlässt sich CA Identity Manager auf die Gerätesicherheit anstelle von Sicherheitsfragen. Möglicherweise muss die Gerätesicherheit erhöht werden, zum Beispiel durch einen Passcode, bevor Sie die Funktion zum Rücksetzen von Kennwörtern aktivieren.

- Ändern eines Kennworts
- Reagieren auf Genehmigungsanforderungen
- Anzeigen von Managerdetails

  Diese Funktion erlaubt Benutzern, die Workflow-Anfragen genehmigen, Informationen zum Vorgesetzten (Manager) eines Benutzers anzuzeigen.

Hinweis: Version 1.0 der mobilen App wird von CA Identity Manager 12.6.5 nicht unterstützt. Laden Sie die aktuelle Version im Apple Store herunter.

Weitere Informationen zur mobilen App finden Sie im *Administrationshandbuch*.

Synchronization/Remove Account Template Values From Accounts (Kontenvorlagenwerte synchronisieren oder aus Konten entfernen)

Sie können jetzt die Funktion "Synchronization/Remove Account Template Values From Accounts" (Kontenvorlagenwerte synchronisieren oder aus Konten entfernen) auf dem Attribut "Responsibilities List" (Zuständigkeitsliste) der Oracle Applications-Kontovorlage verwenden, damit eine Zuständigkeitseingabe auf dem Oracle Applications-Konto abläuft.

Zusätzlich enthält diese Version Verbesserungen der Zuständigkeitsberechnungen, um "nicht synchron"-Fehler zu verhindern.

Weitere Informationen über die Funktion finden Sie unter Responsibilities List and Account Synchronization (Zuständigkeitsliste und Kontosynchronisierung) im *Connectors-Handbuch*.

Erweiterte Konfigurationen für den LND-Connector

Um die Leistung des LND-Connectors während der Vorgänge "Durchsuchen und Korrelieren" zu verbessern, sind nun folgende konfigurierbare Einstellungen verfügbar:

- readExpirationDateInSearch
- readOuFromPrimaryAddressBookOnly
- readAcctFromPrimaryAddressBookOnly
- enableUouDetection

Hinweis: Sie können die Werte der obigen Attribute in der folgenden Datei ändern:

```
CA\Identity Manager\Connector Server\conf\override\lnd\connector.xml
```

Schema der Aufgabenpersistenz-Datenbank

Diese Version enthält Verbesserungen für SQL-Skripte, die das Aufgabenpersistenz-DB-Schema aktualisieren. Die Skripte legen die richtige Spaltengröße fest und fügen die Prozedur ein, die in den Statusdetails der Laufzeit gespeichert sind.

In dieser Aktualisierung sind keine Größendiskrepanzen zwischen der runtimeStatusDetail12-Tabelle und der entsprechenden archive_runtimeStatusDetail12-Tabelle für neue oder aktualisierte Systeme vorhanden. Diese Aktualisierung beseitigt die Fehler mit der Aufgabe "Gesendete Aufgaben bereinigen".

Unterstützung für das Deaktivieren des SAP-Kontokennworts

In dieser Version ist das Attribut "Kennwort deaktiviert" jetzt auf der Registerkarte "Konto" verfügbar. Mithilfe dieses Attributs können Sie ein SAP-Konto mit einem deaktivierten Kennwort erstellen. Sie können auch das Kennwort eines vorhandenen SAP-Kontos deaktivieren. Setzen Sie das Administratorkennwort zur erneuten Aktivierung zurück.

Zwei Modi für das Verbinden mit Exchange: Agentless und Agent

Mit dieser Version können Sie eine Verbindung mit Exchange 2007- und Exchange-2010-Endpunkten herstellen, ohne dabei einen Agenten zu verwenden. Wir empfehlen, dass Sie den Agentless-Modus für neue Verbindungen zu diesen Endpunkten verwenden.

Allerdings funktioniert der Agentless-Modus nicht mit Exchange 2003, und Sie müssen die Verbindung mithilfe des Remote-Agenten herstellen.

Folgende Tabelle listet die unterstützten Exchange-Versionen für Agent- und Agentless-Modi auf:

Endpunktversionen	Agent	Agentless
Exchange 2003	Ja	Nein
Exchange 2007	Ja	Ja
Exchange 2003 und Exchange 2007	Ja	Nein
Exchange 2010	Ja	Ja
Exchange 2007 und Exchange 2010	Ja	Ja

Unterstützung für Exchange Data Access Groups (DAG)

Exchange 2010 kann in dieser Version DAGs (Data Access Groups) verwenden, um die Hochverfügbarkeit sicherzustellen. Sie können eine Verbindung zu DAG herstellen, um sicherzustellen, dass die Verbindung zum Endpunkt einen Failover übersteht.

Unterstützung für Automatic Mailbox Distribution in Exchange 2010

In dieser Version kann der Active Directory (AD) Exchange-Connector eine automatische Postfachverteilung in Exchange 2010 verarbeiten.

Wenn Sie ein Postfach oder MailEnable erstellen oder zu einem vorhandenen Benutzer verschieben, dann muss das Postfach in einer Postfachdatenbank gespeichert werden. Für frühere Exchange-Server ist es erforderlich, dass Sie die Postfachdatenbank für die Ausführung von einem der oberen Vorgänge angeben. Exchange Server 2010 wählt die Datenbank mithilfe der automatischen Postfachverteilung aus.

Verbindung mit SQL Server, wenn die Datenbank offline ist

Sie können jetzt einen SQL Server-Endpunkt durchsuchen und korrelieren, wenn die zugehörige Datenbank offline ist.

Aufgabe zur Erstellung einer Snapshot-Definition für Berichte

Wir empfehlen jetzt, dass Sie die Aufgabe "Snapshot-Definition erstellen" verwenden, um einen Snapshot für die Daten zu erstellen, die für das Erstellen eines Berichts erforderlich sind. Die standardmäßigen Snapshot-XML-Parameterdateien werden ersetzt. Weitere Informationen finden Sie im *Administrationshandbuch*.

12.6.1

Neue Zertifizierungen

Die folgenden neuen Plattformen sind mit CA Identity Manager r12.6.1 zertifiziert:

Endpunkte

- Microsoft SQL 2012 als statischer und dynamischer Endpunkt
- CA Directory r12 SP10 CR2 als JNDI-Endpunkt
- CA Embedded Entitlements Manager (EEM) - unterstützt vom Bereitstellungsmanager

CA Identity Manager-Benutzerspeicher

- CA Directory r12 SP10 CR2

CA Identity Manager-Benutzerspeicher und Laufzeitspeicher

- Microsoft SQL Server 2012 SP1

Zusätzliche Unterstützung

- Mozilla Firefox 14.x
- BusinessObjects Report Server XI 3.1 SP5 (CA Business Intelligence 3.3)

  Diese Version stimmt mit der von CA SiteMinder unterstützten Version überein
- Unterstützung des Report Server in Hochverfügbarkeitskonfigurationen
- Unterstützung für CA Identity Manager mit CA Identity Governance r12.6
- Unterstützung für CA Identity Manager mit CA SiteMinder r12.0 SP3 CR11

SSL-fähiger JNDI-Benutzerspeicher

Peer-Zertifikatsprüfung wird derzeit durchgeführt. Bei dieser Funktion müssen Sie das SSL-Serverzertifikat des Benutzerspeichers dem CA Identity Manager-JRE-Standardschlüsselspeicher hinzufügen. Der Schlüsselspeicher ist die Cacerts- oder Jssecacerts-Datei an folgendem Speicherort:

JAVA_HOME\jre\lib\

Verwenden Sie das Keytool des JDK-Hilfsprogramms, um das Zertifikat hinzuzufügen.

Unterstützung für verschlüsselte Kennwörter im Bootstrap-Verzeichnis der Management-Konsole

Wenn Sie die Management-Konsole mithilfe des Bootstrap-Verzeichnisses "AuthenticationDirectory" sichern, können Sie nun das Kennwort für den Administrator der Management-Konsole verschlüsseln.

12.6

Neuer Name und Anzeige

Zusätzlich ist die Standardbenutzerkonsole aktualisiert worden, um neue CA-Stile und -Farben wiederzugeben.

Java Connector Server (Java CS oder JCS) wurde in CA IAM Connector Server umbenannt (CA IAM CS).

Vereinfachte Benutzererfahrung

Diese Version schließt die folgenden Verbesserungen an der Benutzererfahrung ein:

- Aktualisierte Fenster für Self-Service-Aufgaben

  Die folgenden Fenster wurden aktualisiert, um die Benutzerfreundlichkeit zu verbessern:

  - Erscheinungsbild des Portals für das Anmeldefenster
  - Selbstregistrierung/Erstellung von Identität
  - Mein Kennwort ändern
  - Kennwort vergessen – Zurücksetzen
  - Benutzer-ID vergessen

- Bestimmte Admin-Aufgaben nutzen Web 2.0-Steuerelemente.

Bereitstellungs-Verbesserungen

CA Identity Manager 12.6 schließt die folgenden neuen Funktionen und Änderungen zur Verbesserung der Bereitstellung ein.

Bereitstellungsserver unter Linux

Der Bereitstellungsserver kann jetzt unter Red Hat Linux als eine Alternative zu Solaris installiert werden.

Funktionen des Bereitstellungsmanagers in der Benutzerkonsole

Einige Funktionen des Bereitstellungsmanagers werden jetzt in der Benutzerkonsole unterstützt:

- Synchronisierung von Benutzern, Rollen, Endpunktkonten und Kontovorlagen

  Die Integration von Endpunkten und Konten in CA Identity Manager kann zu Verlusten bei der Synchronisierung führen. Beispielsweise können sich die Bereitstellungsrollen oder Kontovorlagen, die einem Benutzer zugewiesen werden, von den tatsächlichen Konten für diesen Benutzer unterscheiden. Dieses Problem kann mit Synchronisierungsaufgaben behoben werden.

- Korrelationsregeln steuern die Zuordnung von Endpunktkontoattributen zu Benutzerattributen in der Benutzerkonsole. So hat beispielsweise Access Control ein Attribut namens "AccountName". Sie können eine Regel erstellen, um es "FullName" in der Benutzerkonsole zuzuordnen.

Connector-Verbesserungen

CA Identity Manager 12.6 schließt die folgenden neuen Funktionen und Änderungen ein, mit deren Hilfe sich die Erstellung und Bereitstellung neuer Connectors vereinfacht.

Hot Deployment – Installieren eines neuen Connector ohne Neustart von CA IAM CS

CA IAM Connector Server (CA IAM CS) ist der neue Name für Java Connector Server (oder Java CS oder JCS).

CA IAM CS unterstützt jetzt *Hot Deployment*. Hot Deployment ist ein Prozess, mit dessen Hilfe eine Komponente ohne Neustart von CA IAM CS hinzugefügt, entfernt oder aktualisiert werden kann. Sie können jetzt die folgenden Aufgaben ausführen:

- Installieren, Deinstallieren oder Upgraden eines Connector *ohne* Neustart von CA IAM CS

  Sie können einen neuen oder aktualisierten Connector bereitstellen und installieren, ohne CA IAM CS neu zu starten oder sich bei seinem Host anzumelden. Wenden Sie sich an den CA Support für die neuesten Connector-Versionen.

- Bereitstellen von Bibliotheken anderer Anbieter ohne Neustart von CA IAM CS

  Einige Connectors benötigen Bibliotheken, die nicht im Lieferumfang von CA IAM CS sind. Bisher mussten Sie diese Bibliotheken bereitstellen und dann CA IAM CS neu starten. Jetzt können Sie diese Bibliotheken bereitstellen, während der Connector-Server ausgeführt wird.

  CA IAM CS enthält einen Kernsatz von Bibliotheken anderer Anbieter, und jeder Connector kann jede dieser Bibliotheken verwenden. Ein Connector kann auch andere Bibliotheken von Drittanbietern enthalten, die er benötigt.

Hinweis: Hot Deployment funktioniert nicht für C++-Connectors.

Bundle Builder – Neues Tool für das Erstellen von Connectors

CA IAM CS erfordert, dass Connectors als Open Services Gateway Initiative-Bundles geliefert werden. Das OSGi-Framework ist ein Modulsystem und eine Service-Plattform für die Java-Programmiersprache, die ein vollständiges und dynamisches Komponentenmodell implementiert. Das SDK für den Connector-Server schließt jetzt ein Bundle Builder-Tool ein, das Ihnen dabei hilft, Ihren Connector mit einem Bundle zu umgeben.

Anmelden für Connectors und CA IAM CS

Sie können sich jetzt bei CA IAM CS anmelden, um aktuellste Protokollmeldungen für CA IAM CS und seine Connectors zu sehen. Sie können weiterhin Protokolldateien verwenden, um alle Protokollmeldungen zu sehen.

Zertifikate für Connectors und CA IAM CS

Sie können sich jetzt bei CA IAM CS anmelden, um Zertifikate für CA IAM CS und seine Connectors anzuzeigen und zu verwalten.

Verwenden von Connector Xpress zum Zuordnen von benutzerdefinierten Attributen zu benutzerdefinierten Funktionsattributen

Verwenden Sie Connector Xpress, um benutzerdefinierte Attribute und benutzerdefinierte Funktionsattribute zuzuordnen. Die Zuordnung der Attribute kann nicht mehr über die XML-Datei "<jcs-home>/conf/override/lnd/lnd_custom_metatdata.xml" vorgenommen werden.

CA IAM CS ist ein Proxy für CCS

CA Identity Manager verwendet jetzt CA IAM CS als einen Proxy für den C++ Connector Server (CCS). CA Identity Manager kommuniziert nicht mehr direkt mit CCS.

Leistungs-Verbesserungen

CA Identity Manager 12.6 bietet Leistungsverbesserungen in folgenden Bereiche des Produkts.

Verbesserung der Leistung des Massendatenladers

In dieser Version ist die Leistung des Massendatenladers verbessert. Die Verbesserungen schließen die folgenden Änderungen ein:

- Höhere Übermittlungsrate von Aufgaben durch die übergeordnete Massendatenlader (Feeder)-Aufgabe. Es können mehr Aufgaben parallel ausgeführt werden.
- Optimierungen bei der Wiederverwendung von Datenbankverbindungen; Zwischenspeicherung der Attributdefinitionen von verwalteten Objekten führt von Anfang bis Ende zu einer schnelleren Ausführung von Aufgaben.
- Verbesserungen an einigen Plug-ins und Listenern beschleunigt die Verarbeitung von Ereignissen, die während der Aufgabenausführung generiert werden.

Um die Leistung weiter zu verbessern, empfehlen wir, dass Sie für die Dauer des Massendatenladevorgangs folgende Änderung vornehmen:

- Deaktivieren Sie alle unerwünschten Policy Xpress-Richtlinien, Business Logic Task-Handler und Synchronisierungs-Flags auf Aufgabenebene.
- Führen Sie den Massendatenlader (Feeder) als dedizierter Benutzer mit möglichst wenigen Admin-Rollen und Admin-Aufgaben in Bereich aus.

Hinweis: Weitere Informationen zu zusätzlichen Leistungsverbesserungen finden Sie im Abschnitt zum Massendatenlader im *Administrationshandbuch*.

Verbesserte Snapshot-Exportleistung

Für diese Version wurde der Exportprozess von Snapshot-Daten für Berichte umgestaltet, um die Leistung und Benutzerfreundlichkeit zu verbessern. Mithilfe des Snapshot-Definitionsassistenten können Sie die Regeln zum Laden von Benutzern, Endpunkten, Admin-Rollen, Bereitstellungsrollen, Gruppen und Organisationen definieren oder anpassen.

Mithilfe dieser Funktion können Sie eine Benutzerkonsolen-Aufgabe verwenden, um nur die gewünschten Attribute auszuwählen und für eine bestimmte Snapshot-Instanz zu exportieren. In früheren Versionen mussten Benutzer eine XML-Datei manuell bearbeiten.

Hinweis: Sie können weiterhin die Standard-XML-Dateien für das Erfassen von Snapshots verwenden und anpassen.

Weitere Informationen zum Erstellen von Snapshot-Definitionen finden Sie im *Administrationshandbuch*.

Policy Xpress-Verbesserungen

Diese Version enthält die folgenden Verbesserungen von Policy Xpress:

- Attribut-Plug-ins für verwaltete Objekte

  Die folgenden Plug-ins für verwaltete Objektattribute sind zu Policy Xpress hinzugefügt worden:

  - Objekt Attribute – Erlauben Ihnen, den Wert eines verwalteten Objektattributs zu extrahieren.
  - Mit geändertem Objektattributwert/Attribut eines bestimmten Objekts – Wie "Mit geändertem Objektattributwert" und "Attribut eines bestimmten Benutzers", aber es kann jeder Typ von verwaltetem Objekt verwendet werden
  - Set Objekt Attribut – Erlaubt Ihnen, das Attribut von verwalteten Objekten zu ändern

- Kürzungsfunktion

  Die Kürzungsfunktion ermöglicht es Ihnen, unerwünschte voran- oder nachgestellte Bereiche aus Datenelementen oder Zeichenfolgen zu entfernen.

- Unterstützung für weitere Aktionsregeln

  Bisher konnten einer Richtlinie nicht mehr als 60–70 Aktionsregeln hinzugefügt werden, sonst hat Policy Xpress die ganze Richtlinie nicht hinzugefügt. In diesem Fall wurden weder ein Fehler noch eine Ausnahme in den Protokollen berichtet. Jetzt unterstützen Policy Xpress-Richtlinien bis zu 500 Aktionsregeln.

- Policy Xpress-Wiki

  Die Policy Xpress-Dokumentation wurde aktualisiert und befindet sich nun auf einem Wiki in der CA Security Global User Community.

Sichere Management-Konsole

Die Management-Konsole ermöglicht Administratoren, CA Identity Manager-Verzeichnisse und -Umgebungen zu erstellen und zu verwalten.

Die CA Identity Manager-Installation enthält nun eine Option, die standardmäßig aktiviert ist und die der Sicherung der Management-Konsole dient. Während der Installation erstellen Sie ein Konto, das auf die Management-Konsole in einem vordefinierten Verzeichnis zugreifen kann.

Nach der Installation können Sie der Management-Konsole zusätzliche Administratoren hinzufügen, die einen Zugriff benötigen.

Hinweis: Weitere Informationen finden Sie im *Konfigurationshandbuch*.

Basiszugriffsanfragen

CA Identity Manager-Benutzer können Zugriff auf Dienste anfordern, die sie zur Ausführung ihrer Arbeitsaufgaben benötigen.

Ein *Dienst* bündelt alle Berechtigungen (Aufgaben, Rollen, Gruppen und Attribute), die ein Benutzer für eine bestimmte Unternehmensrolle benötigt. Services sind für den Benutzer über Zugriffsanfrage-Aufgaben in der CA Identity Manager-Benutzerkonsole verfügbar. Zugriffsanfrage-Aufgaben ermöglichen einem Benutzer oder Administrator, einen Service anzufordern, zuzuweisen, zu widerrufen und zu erneuern.

Dienste ermöglichen einem Administrator, Benutzerberechtigungen in einem einzigen Paket zu kombinieren, die dann als ein Set verwaltet werden. Zum Beispiel benötigen alle neuen Vertriebsmitarbeiter Zugriff auf einen definierten Satz von Aufgaben und auf Konten von bestimmten Endpunktsystemen. Sie benötigen auch bestimmte Informationen, die zu ihren Benutzerkontoprofilen hinzugefügt wurden. Ein Systemadministrator erstellt einen Service namens Vertriebsverwaltung, der alle erforderlichen Aufgaben, Rollen, Gruppen und Profilattributinformation für einen neuen Vertriebsmitarbeiter enthält. Wenn ein Administrator den Service "Vertriebsverwaltung" einem Benutzer zuweist, erhält dieser Benutzer die gesamte Gruppe an Rollen, Aufgaben, Gruppen und Kontoattributen, die vom Service definiert werden.

Eine weitere Möglichkeit, wie Benutzer auf Services zugreifen können, ist mit einer eigenen Zugriffsanfrage. In der Benutzerkonsole hat jeder Benutzer eine Liste von Services, die für seine Anfrage verfügbar sind. Diese Liste wird mit Services gefüllt, die von einem Administrator mit den entsprechenden Berechtigungen als "Selbstabonnierend" markiert wurden, normalerweise während der Service-Erstellung. Über die Liste der verfügbaren Services können Benutzer den Zugriff auf die benötigten Services anfordern. Wenn der Benutzer Zugriff auf einen Service anfordert, wird die Anfrage automatisch erfüllt, und die zugeordneten Berechtigungen werden dem Benutzer sofort zugewiesen. Ein Administrator mit den entsprechenden Berechtigungen kann die Service-Abwicklung auch so konfigurieren, dass eine Workflow-Genehmigung erforderlich ist oder E-Mail-Benachrichtigungen generiert werden.

Hinweis: Diese Anfangsversion unterstützt Funktionen für Basiszugriffsanfragen. Die Zugriffsanforderungs-Funktionalität ermöglicht Endbenutzern, Berechtigungen anzufordern (verwaltet und nicht verwaltet von CA Identity Manager), Genehmigungsabläufe zu definieren und Abwicklungsabläufe zu verwenden.

Diese Anfangsversion bietet keine Unterstützung für erweiterte Zugriffsanforderungsfunktionen wie

- Massendefinition von Zugriffsanforderungs-Dienstobjekten
- Integration mit CA Identity Governance (früher als CA GovernanceMinder bezeichnet)
- Detailliertes Filtern und Suchen

Diese Anfangsversion bietet keine Unterstützung von folgenden Funktionen:

- Massendefinition von Dienstobjekten
- Detaillierte Filterung
- Suchen
- Integration von anderen Abwicklungsmechanismen

Weitere Informationen zu Diensten finden Sie im *Administrationshandbuch*.

Neue Dokumentation für Config Xpress

Config Xpress ist ein Tool, das mit CA Identity Manager bereitgestellt wird. Sie können dieses Tool verwenden, um die Konfigurationen Ihrer CA Identity Manager-Umgebungen zu analysieren und um mit diesen Konfigurationen zu arbeiten.

Config Xpress ermöglicht es Ihnen, folgende Aufgaben auszuführen:

- Verschieben von Komponenten zwischen Umgebungen.

  Das Tool entdeckt automatisch andere erforderliche Komponenten und fordert Sie auch dazu auf, diese zu verschieben. Dies kann Ihnen viel Arbeit ersparen.

- Veröffentlichen eines Berichts zu den Systemkomponenten in einer PDF-Datei.
- Veröffentlichen der XML-Konfiguration einer bestimmten Komponente.

Weitere Informationen zum Importieren von Konfigurationen finden Sie unter Verwalten der Konfiguration im *Konfigurationshandbuch*.

Systemeigener CA Identity Manager-Ersatz für SiteMinder Advanced Password Services

Zusätzlich zu den grundlegenden Kennwortrichtlinien bietet CA Identity Manager die folgenden zusätzlichen Kennworteinstellungen, die nun von SiteMinder abgekoppelt sind:

- Ablauf des Kennworts:
  - Verfolgen von fehlgeschlagenen oder erfolgreichen Anmeldungen – Wenn die Option aktiviert ist, werden Nachverfolgungsinformationen für erfolgreiche oder fehlgeschlagene Anmeldeversuche zum Kennwortdatenattribut des dazugehörigen Benutzers im Benutzerspeicher geschrieben.
  - Authentifizieren von Anmeldungsnachverfolgungsfehler – Wenn die Option deaktiviert ist, können sich Benutzer nur anmelden, wenn CA Identity Manager Nachverfolgungsinformationen in den Benutzerspeicher schreiben kann.
  - Kennwort läuft ab, wenn es nicht geändert wird – Konfiguriert das Verhalten bei Ablauf. Wenn das Kennwort nach einer angegebenen Anzahl von Tagen nicht geändert wurde, werden Benutzer deaktiviert oder gezwungen, ihr Kennwort zu ändern. Erlaubt auch das Senden von Ablaufwarnungen nach einer angegebenen Anzahl von Tagen.
  - Kennwort-Inaktivität – Konfiguriert inaktives Benutzerverhalten. Wenn der Benutzer nach einer angegebenen Anzahl von Tagen keinen erfolgreichen Anmeldeversuch unternommen hat, werden Benutzer deaktiviert oder gezwungen, ihr Kennwort zu ändern.
  - Ungültiges Kennwort – Konfiguriert die Anzahl von fehlgeschlagenen Anmeldungen, die erlaubt sind, bevor der Benutzer deaktiviert wird.
  - Mehrere reguläre Ausdrücke – Gibt reguläre Ausdrücke an, mit denen Kennwörter übereinstimmen müssen bzw. nicht übereinstimmen dürfen. CA Identity Manager-Kennwortrichtlinien unterstützen einen einzelnen Ausdruck von jedem Typ.
- Beschränkungen für Kennwort:
  - Mindestanzahl von Tagen vor Wiederverwendung
  - Mindestanzahl von Kennwörtern vor Wiederverwendung
  - Prozentualer Unterschied zum letzten Kennwort
  - Bei der Prüfung auf Unterschiede Sequenz ignorieren – Ignoriert beim Berechnen des prozentualen Unterschieds die Position von Zeichen.

Hinweis: Diese Version unterstützt keine historischen Kennwortdaten einer CA Identity Manager-Bereitstellung, die CA SiteMinder Password Services (Kennwortverlauf) für Bereitstellungen verwendet, die nur CA Identity Manager r12.6-Kennwortdienste umfasst.

Dynamische Schlüssel für das Verschlüsseln von Daten

In einer Umgebung können Sie dynamische Schlüssel erstellen, die Daten verschlüsseln oder entschlüsseln. Wenn Sie vermuten, dass ein Benutzer unbefugten Zugriff auf einen Schlüssel erhalten hat, können Sie das Kennwort für den Schlüsselspeicher ändern. Der Schlüsselspeicher ist die Datenbank für geheime Schlüssel. Sobald Sie dieses Kennwort ändern, verschlüsselt CA Identity Manager die Werte der Schlüssel wieder.

Weitere Details dazu finden Sie im Abschnitt Geheime Schlüssel verwalten des *Administrationshandbuchs*.

Synchronisierung von Active Directory-Servern

CA IAM CS kann so konfiguriert werden, dass Benutzer mit Active Directory-Server (ADS) lokale Identitätsinformationen mit Cloud-basierten Endpunktinformationen synchronisieren können. Sie können zum Beispiel Ihren ADS so einrichten, dass er mit einer Cloud-basierten SalesForce-Installation synchronisiert wird. Ergänzungen oder Änderungen an einer synchronisierten lokalen Benutzergruppe werden dann zur SalesForce-Umgebung übertragen.

Diese Funktion benötigt CA IAM CS, einen unterstützten Endpunkt und den entsprechenden Connector.

Beachten Sie zur Active Directory-Synchronisierungsfunktion Folgendes:

- Diese Funktion unterstützt nur Active Directory. Andere LDAP-Verzeichnisse werden in dieser Version nicht für die Verwendung mit dieser Funktion unterstützt.
- Diese Funktion unterstützt nur Cloud-basierte Endpunkte, für die ein Connector vorhanden ist. In dieser Version zählen Google Apps und SalesForce zu den unterstützten Anwendungen.

Weitere Informationen zu dieser Funktion finden Sie im *Connectors Guide*.

Auditing von Anmelde- und Abmeldeereignissen

Um die Überwachung des Benutzerzugriffs in der CA Identity Manager-Umgebung zu verbessern, können Sie CA Identity Manager so konfigurieren, dass die Anmelde- und Abmeldeereignisse in einer Umgebung überwacht werden. Sie können diese protokollierten Ereignisse im Standardbericht "Auditdetails" anzeigen.

Hinweis: Benutzeranmelde- und Benutzerabmeldeereignisse können nicht für CA SiteMinder protokolliert werden.

Sie können diese Einstellungen in der Auditeinstellungsdatei konfigurieren. Weitere Informationen zum Konfigurieren von Anmelde- und Abmeldeereignissen finden Sie im Kapitel "Auditing" des *Konfigurationshandbuchs*.

SHA-2

SHA-2-SSL-Zertifikat-Hashing ist ein kryptografischer Algorithmus, der vom National Institute of Standards and Technology (NIST) und der National Security Agency (NSA) entwickelt wurde. SHA-2-Zertifikate sind sicherer als alle vorherigen Algorithmen. In CA Identity Manager können Sie SHA-2-signierte SSL-Zertifikate anstelle von Zertifikaten konfigurieren, die mit der SHA-1-Hash-Funktion signiert wurden.

Kapitel 2: Hinweise zur Installation

Dieses Kapitel enthält folgende Themen:

Policy Xpress-Unterstützung für SOAP- and REST-Webservices aktivieren

Policy XPress wurde erweitert und unterstützt jetzt die Webservices SOAP (mit einfacher Authentifizierung) und REST (mit einfacher Authentifizierung, Proxy-Authentifizierung und OAuth-Authentifizierung), sodass es mit externen Anwendungen integriert werden kann, die mit einer Webservice-Schnittstelle ausgestattet sind. Um die Policy XPress-Webservices (SOAP und REST) mit JBoss 5.1 Community Edition zu verwenden, kopieren Sie die folgenden JAR-Dateien aus dem "client"-Verzeichnis in Ihr JBoss 5.1-Community-Edition-"\lib\endorsed"-Verzeichnis. Starten Sie anschließend den Anwendungsserver neu.

- jbossws-native-jaxrpc.jar
- jbossws-native-jaxws.jar
- jbossws-native-jaxws.jar
- jbossws-native-saaj.jar

Hinweis: Für die EAP-Versionen brauchen diese Dateien nicht kopiert zu werden.

Unterstützte Plattformen und Versionen

In CA CA Identity Manager 12.6.5 wurden an unterstützten Anwendungsserver-Versionen, -verzeichnissen und -datenbanken Änderungen vorgenommen.

Hinweis: Eine vollständige Liste der unterstützten Plattformen und Versionen finden Sie in der CA Identity Manager-Support-Matrix auf der Website von CA Support.

Veraltete und verworfene Komponenten

Bestimmte Komponenten werden als veraltet markiert, was heißt, dass sie in künftigen Versionen nicht mehr unterstützt werden. Andere Komponenten werden verworfen, was bedeutet, dass sie nicht mehr mit dem Produkt geliefert oder nicht mehr mit dem Produkt getestet werden. Diese Komponenten sind in der CA Identity Manager Deprecation Policy bei CA Support aufgelistet.

Co-Installation von Unix-Remote-Agenten mit zusätzlichen CA-Produkten

In dieser Version werden die UNIX-Remote-Agenten (außer TRU64-Plattformen) jetzt so installiert, dass die installierte Software die abhängigen Softwarekomponenten, wie z. B. CA ITCM, verfolgt.

Wenn Sie ein Upgrade der UNIX-Remote-Agenten durchführen möchten, aktualisiert die neue Nachverfolgungsmethode nicht die Referenzanzahl der abhängigen Softwarekomponenten. Wenn Sie das Produkt nach diesem Upgrade deinstallieren möchten, verwenden Sie folgende Deinstallationsdatei:

```
<install-dir>/scripts/uninstall-force.sh
```

Hinweis: Stellen Sie sicher, dass "uninstall-force.sh" nicht auf Hosts verwendet wird, auf denen zusätzliche CA-Software installiert ist. Die Produkte können von den gleichen Softwarepaketen abhängen, die dieses Skript entfernt.

Nicht verschlüsselte Kennwörter

Bei neuen Installationen werden Benutzerkennwörter nicht standardmäßig verschlüsselt. Auch wenn SiteMinder in CA Identity Manager integriert ist, können Sie die Kennwortverschlüsselung nicht mit "AttributeLevelEncrypt" aktivieren. Dieses Attribut funktioniert nur, wenn SiteMinder nicht installiert ist.

Das Problem wird in einer künftigen Version behoben sein.

Oracle Oracle 11g R2 RAC als Benutzerspeicher und Objektspeicher

Bei Verwendung von Oracle 11g R2 RAC als Benutzerspeicher und Laufzeitspeicher müssen Sie Folgendes ausführen, um die Cluster-Funktionen eines Oracle-Datenbank-Clusters verwenden zu können:

- Verwenden Sie SCAN (Single Client Access Name), um CA Identity Manager mit Oracle 11g R2 RAC zu installieren.
- Erstellen Sie den Datenbank-*Tablespace* auf der gemeinsam genutzten Festplattengruppe, während ein Tablespace erstellt wird.

Oracle 12c RDB als Benutzerspeicher und Objektspeicher

Wenn Oracle 12c RDB als Benutzerspeicher und Laufzeitspeicher eingesetzt wird, verwenden Sie nur den DB-Modus ohne Container. Die Container-RDBMS-Option (Mandantenfähigkeit) von Oracle 12c ist im Enterprise-Produkt ausgeschlossen.

ADAM 2008 als Benutzerspeicher

Wenn Sie ADAM 2008 als den CA Identity Manager-Benutzerspeicher benutzen und Sie CA Identity Manager mit SiteMinder integrieren, ist SiteMinder r6.0 SP6/r6.x QMR6 erforderlich.

Nicht-ASCII-Zeichen verursacht Installationsfehler auf nicht englischsprachigen Systemen

Während der Installation von CA Identity Manager extrahiert das Installationsprogramm Dateien in ein Temp-Verzeichnis. Auf einigen lokalisierten Systemen enthält der Standardpfad zum Temp-Verzeichnis Nicht-ASCII-Zeichen. Der Standardpfad zum Temp-Verzeichnis lautet beispielsweise auf spanischen Windows-Systemen:

C:\Documents and Settings\Administrador\Configuración local\Temp

Das Nicht-ASCII-Zeichen sorgt dafür, dass das Installationsprogramm eine leere Übersichtsseite für die Installationsvorbereitungen anzeigt und die Installation anschließend fehlschlägt.

Behelfslösung

Ändern Sie die Tmp-Umgebungsvariable so, dass sie auf einen Ordner verweist, der ausschließlich ASCII-Zeichen enthält.

Umgehen der Firewall unter Windows 2008 SP2

In Windows 2008 SP2-Bereitstellungen wird während der Installation die Kommunikation mit CA Identity Manager-Komponenten wie dem Bereitstellungsserver, dem Java Connector Server und C++-Connector-Server von der Firewall gesperrt.

Fügen Sie Port-Ausnahmen hinzu oder deaktivieren Sie die Windows-Firewall, um in Windows 2008 SP2-Bereitstellungen auf verteilte CA Identity Manager-Komponenten zuzugreifen.

Bereitstellen von JSP-Seiten für Administratoraktionen

Der CA Identity Manager-Server umfasst Beispiel-JSP-Seiten für die Ausführung der folgenden Aktionen:

- Anpingen des Anwendungsservers
- Auflisten der bereitgestellten BLTHs
- Auflisten der Information über Objekttypen und Anbieter von verwalteten Objekten
- Auflisten der Plug-in-Informationen
- Ändern der Protokollierungsebenen

Die JSP-Seiten werden an diesem Speicherort installiert:

admin_tools\samples\admin

Der Ordner enthält eine readme.txt-Datei mit Anweisungen für die Verwendung der JSP-Seiten.

Hinweis: Es wird ein Fehler 404 angezeigt, wenn Sie diese JSP-Seiten verwenden, ohne die Anweisungen in der readme.txt-Datei zu befolgen.

Installation des Bereitstellungsverzeichnisses auf Linux

Wenn Sie das Bereitstellungsverzeichnis auf einem Linux-System installieren, verwendet das System automatisch IPv6-Adressen, auch wenn Sie beabsichtigen, auf diesem System IPv4 zu verwenden. Alle DSAs scheinen zu funktionieren, jedoch könnte beim Versuch, über Jxplorer eine Verbindung zu den DSAs herzustellen, oder den Bereitstellungsserver zu installieren, die Fehlermeldung "Verbindung abgelehnt" angezeigt werden.

So deaktivieren Sie IPv6 auf Linux

1. Folgen Sie vor der Installation des Bereitstellungsverzeichnisses den Schritten des Red Hat Knowlegde Base-Artikels unter IPv6 auf LINUX deaktivieren.
2. Vergewissern Sie sich, dass die Datei "/etc/hosts" keinen Eintrag für folgende Adresse hat:

   127.0.0.1 *hostname*

Linux: JDK-Anforderung für Installation

CA Identity Manager 12.6.5 benötigt Oracle JDK 1.6.

RedHat 6.x enthält OpenJDK 1.6, was dazu führen kann, dass das CA Identity Manager-Installationsprogramm hängen bleibt. Stellen Sie sicher, dass Sie die in der CA Identity Manager-Unterstützungsmatrix angegebene Sun JDK-Version verwenden.

CA Identity Manager auf Linux 64-Bit mit SiteMinder-Konnektivitätsfehlern

Das Installationsprogramm berichtet Fehler bei CA Identity Manager auf Linux 64-Bit, wenn die Option "Verbindung zum SiteMinder herstellen" ausgewählt wurde. Die erforderliche Agentenkonfiguration ist in SiteMinder nicht korrekt

Wichtig! Führen Sie vor der Bereitstellung eines Verzeichnisses oder einer Umgebung die Behelfslösungsschritte durch.

Behelfslösung

1. Rufen Sie den Agentenamen und das Kennwort ab, die Sie bei der Installation angegeben haben. Alternativ können Sie den Wert für die "AgentName"-Eigenschaft folgender Datei entnehmen:

   ```
   \iam_im.ear\policyserver.rar\META-INF\ra.xml
   ```

2. Öffnen Sie die SiteMinder WAM-Benutzeroberfläche und erstellen Sie einen Agenten mit dem Agentennamen. Aktivieren Sie ganz bewusst das Kontrollkästchen "4.x-Agent".

3. Starten Sie den Anwendungsserver und vergewissern Sie sich, dass keine Konnektivitätsprobleme beim Richtlinienserver auftreten.

   Es sollte eine Zeile wie folgende ohne Ausnahmen angezeigt werden:

   ```
   13:40:43,156 WARN [Standard] * Startschritt 2: Versucht, PolicyServerService
   zu starten
   ```

Verbessern der Leistung bei WebSphere und AIX

Bei einer WebSphere-Installation unter AIX können Sie die Leistung verbessern, indem Sie in der Benutzerkonsole die größtmögliche Heap-Größe festlegen.

Gehen Sie wie folgt vor:

1. Suchen Sie die Datei "server.xml" an folgendem Speicherort:
   `WAS_HOME/profiles/`*`Profile`*`/config/cells/`*`Cell`*`/nodes/`*`Node`*`/servers/`*`Server`*

2. Fügen Sie im "jvmEntries"-Element Folgendes hinzu: maximumHeapSize="1000".

   Sie können bei Bedarf auch einen höheren Wert verwenden. Um zum Beispiel maximumHeapSize auf 2 GB (2.048 MB) einzustellen, fügen Sie es so hinzu, wie im folgenden Auszug aus dieser Datei fett angezeigt:

```
<jvmEntries xmi:id="JavaVirtualMachine_1183122130078"
verboseModeClass="false"
   verboseModeGarbageCollection="false" maximumHeapSize="2048"
verboseModeJNI="false" runHProf="false" hprofArguments="
debugMode="false" debugArgs="-
agentlib:jdwp=transport=dt_socket,server=y,suspend=n,address=77
77" genericJvmArguments="">
      <systemProperties xmi:id="Property_1"
name="com.ibm.security.jgss.debug" value="off"
required="false"/>
      <systemProperties xmi:id="Property_2"
name="com.ibm.security.krb5.Krb5Debug" value="off"
required="false"/>
    </jvmEntries>
```

Ignorieren von WebSphere 7/Oracle-Fehlern

Wenn CA Identity Manager mithilfe eines Oracle-Laufzeitspeichers und der WebSphere 7 Standard JRE installiert wird, wird in den CA Identity Manager-Protokollen folgender Fehler angezeigt.

> Oracle does not support the use of version 10 of their JDBC driver with the version of the Java runtime environment that is used by the application server.

Dieser Fehler kann ignoriert werden.

Kapitel 3: Upgrades

Folgende Probleme hängen in CA Identity Manager r12.5 SP1 mit Upgrades zusammen.

Dieses Kapitel enthält folgende Themen:

System-Manager-Rolle benötigt Admin-Rollen-Bereich nach Upgrade von 12.6

Nach einem Upgrade von CA Identity Manager, Version 12.6 oder höher, muss der System-Manager-Rolle der Admin-Rollen-Bereich zugeteilt werden.

Hinweis: Wird dies nicht gemacht, gibt eine Suche nach Admin-Rollen möglicherweise keine Ergebnisse zurück.

Führen Sie einen dieser Schritte durch:

- Klicken Sie in der Management-Konsole auf System-Manager und wählen Sie dann den Benutzer aus.
- Oder fügen Sie den Admin-Rollen-Bereich zur System-Manager-Rolle mithilfe von "Admin-Rolle ändern", "System-Manager" hinzu.

Unterstützte Upgrade-Pfade

Sie können ein Upgrade von folgenden Versionen auf CA Identity Manager 12.6.5 durchführen:

- CA Identity Manager r12
- CA Identity Manager r12.5 oder 12.5 SPx
- CA Identity Manager r12.6 oder 12.6 SPx

Wenn Sie CA Identity Manager mit einer Version älter als r12 haben, müssen Sie zuerst ein Upgrade auf r12, r12.5 oder r12.5 SP1 bis SP6 durchführen. Diese Versionen enthalten das Imsconfig-Tool, das erforderlich ist, um ein Upgrade mit einer Version älter als r12 durchführen zu können. Danach können Sie das Upgrade auf CA Identity Manager 12.6.5 durchführen.

Neue Skripte zur Aktualisierung der Aufgabenpersistenz und Archivschemen

Diese Version enthält neue Skripte zur Aktualisierung der Aufgabenpersistenz und Archivschemen. Die Aktualisierung wird automatisch ausgeführt, wenn Sie CA Identity Manager nach einem Upgrade zum ersten Mal starten. Weitere Informationen über die neuen Skripte finden Sie im *Installationshandbuch*.

Neue JCO-Dateien für SAP R3

Wenn Sie den neuen Connector für SAP R3 verwenden möchten, müssen Sie die JCO-Dateien aktualisieren. Weitere Informationen finden Sie im Endpunkthandbuch für den SAP R3-Connector.

Neue Active Directory-Rollendefinitionsdatei

Stellen Sie sicher, dass Sie die neue Rollendefinitionsdatei für Active Directory in jede Umgebung importieren. Die aktuelle CA Identity Manager-Umgebung kann eine frühere Version der Active Directory-Rollendefinitionsdatei haben. Importieren Sie in diesem Fall die Datei, um ein Upgrade der Rollendefinitionen auf 1.08 durchzuführen. Weitere Details zum Importieren von Rollendefinitionsdateien finden Sie in den im *Upgrade-Handbuch* beschriebenen Verfahren.

Aktualisieren auf die Datei "jboss.xml"

Während eines JBoss-Neustarts oder bei der Initialisierung von CA Identity Manager werden zahlreiche Fehlermeldungen in der CA Identity Manager-Datei "server.log" protokolliert. Diese Meldungen beziehen sich auf von JMX verwaltete Ereignisse, aber der empfangende Message Bean ist noch nicht initialisiert. Um dieses Problem zu beheben, enthält die folgende Datei jetzt eine Abhängigkeitsklausel:

```
iam_im.ear\iam_im_identityminder_ejb.jar\META-INF\jboss.xml
```

Die Abhängigkeitsklausel ist in diesem Abschnitt enthalten:

```
<message-driven>
<ejb-name>SubscriberMessageEJB</ejb-name>
<destination-jndi-
name>queue/iam/im/jms/queue/com.netegrity.ims.msg.queue
</destination-jndi-name>
<depends>jboss.web.deployment:war=/iam/im</depends>
</message-driven>
```

Stellen Sie sicher, dass dieser Abschnitt in Ihrer "jboss.xml"-Datei enthalten ist. Das Ergebnis ist, dass die empfangende Message Bean initialisiert wird, bevor JMX beginnt, die Ereigniswarteschlange zu verarbeiten.

64-Bit-Anwendungsserver

CA Identity Manager 12.6.5 unterstützt 64-Bit-Anwendungsserver, die eine bessere Leistung als 32-Bit-Anwendungsserver bieten. Die folgenden Versionen von 64-Bit-Anwendungsservern werden unterstützt:

- JBoss 5.0, 5.1 und 6.1 Enterprise Application Platform (EAP)
- JBoss 5.1 Open Source
- Oracle WebLogic 11g (10.3.5)
- IBM WebSphere 7.0, 8.0, 8.5

Weitere Informationen zur Durchführung eines Upgrades auf Ihrem Anwendungsserver finden Sie im *Upgrade-Handbuch*.

Problem beim Upgrade eines Clusters von CA Identity Manager r12 CR6 oder einer späteren Version

Wenn Sie ein Upgrade an einem Cluster von CA Identity Manager r12 CR6 oder einer späteren Version auf CA Identity Manager r12.5 SP1 vornehmen, schlägt das Upgrade möglicherweise fehl, da manche Cluster-Eigenschaften in der Installationsdatei gelöscht wurden.

Behelfslösung

Stellen Sie vor dem Upgrade sicher, dass folgende Eigenschaften in der Datei "im-installer.properties" vorhanden sind:

- WebSphere: Überprüfen Sie, ob der Cluster-Name in DEFAULT_WAS_CLUSTER angegeben ist. Wenn dies nicht der Fall ist, geben Sie ihn manuell ein.
- WebLogic: Überprüfen Sie, ob der Cluster-Name in DEFAULT_BEA_CLUSTER angegeben ist. Wenn dies nicht der Fall ist, geben Sie ihn manuell ein.

Hinweis: Dieses Problem betrifft kein JBoss-Cluster.

Standardmäßig befindet sich die Installationsdatei an folgenden Speicherorten:

- Windows: C:\Program Files\CA\CA Identity Manager\install_config_info\im-installer.properties
- Unix: /opt/CA/CA_Identity_Manager/install_config_info/im-installer.properties

Workflow-Fehler nach einem Upgrade von Pre-12.5 SP7

Symptom:

Wenn Sie auf dem WebLogic-Anwendungsserver ein Upgrade von einem Pre-r12.5 SP7-System oder älter durchführen möchten, sehen Sie diesen Fehler beim Workflow-Start:

```
WARN  [ims.default] * Startup Step 25 : Attempting to start SchedulerService
ERROR [ims.bootstrap.Main] The IAM FW Startup was not successful
ERROR [ims.bootstrap.Main] org.quartz.SchedulerException: JobStore class
'org.quartz.impl.jdbcjobstore.JobStoreCMT' props could not be configured.
[See nested exception: java.lang.NoSuchMethodException: No setter for
property 'lockHandler.class']
```

Lösung:

1. Halten Sie WebLogic an.
2. Gehen Sie zum Ordner "<IAM-EAR>/APP-INF/lib".
3. Entfernen Sie die folgenden Dateien:
   - common-pool-1.3.jar
   - annotations.jar
   - eurekifyclient.jar
   - quartz-all-1.5.2.jar
4. Starten Sie den Anwendungsserver.
5. Der Workflow-Startfehler wird nicht mehr angezeigt.

Fehler bei der Umgebungsmigration

Symptom:

Wenn Sie ein Upgrade von CA Identity Manager r12 CR1, CR2 oder CR3 vornehmen, kann beim Importieren Ihrer Umgebungen folgender Fehler auftreten:

Das Attribut "accumulateroleeventsenabled" darf nicht im Element "Provisionierung" auftreten.

Lösung:

Öffnen Sie die Datei "envsettings.xml" im exportierten Env.zip und aktualisieren Sie "accumulateroleeventsenabled" auf "acumulateroleeventsenabled" (entfernen Sie das zweite 'c' in 'accumulate').

Upgrade-Fehler von Credential Provider

Nachdem Sie ein Upgrade des Credential Providers für CA Identity Manager r12 auf einer 32-Bit-Windows-Plattform durchgeführt haben, ist das Kontrollkästchen "Anmeldeinformationsanbieter für das Kennwort deaktivieren" in der CAIMCredProvConfig-Anwendung deaktiviert.

Behelfslösung

Öffnen Sie die CAIMCredProvConfig-Anwendung, und aktivieren Sie das Kontrollkästchen.

Interner Fehler des Vista Credential Providers

Symptom:

Beim Upgrade von CA Identity Manager Vista Credential Provider auf 64-Bit-Windows-Plattformen wird die Fehlermeldung *Interner Fehler 2324.2* angezeigt.

Lösung:

Es ist keine Aktion erforderlich, da der Aktualisierungsvorgang erfolgreich abgeschlossen wurde.

Kein Suchfenster mit der Aufgabe "Durchsuchen und Korrelieren"

Wenn Sie CA Identity Manager r12 *oder* CA Identity Manager r12.5 aktualisiert haben *und* die Aufgabe "Durchsuchen und Korrelieren" in das neue Wiederholungsmodell migriert haben, funktioniert die Schaltfläche "Durchsuchen" der Aufgabe "Durchsuchen und Korrelieren" nicht richtig.

Behelfslösung

Konfigurieren Sie ein Suchfenster für die Aufgabe, damit die neue "Durchsuchen"-Schaltfläche ein Suchfenster anzeigt, wenn man auf sie klickt.

Nicht schwerwiegender Fehler nach dem Upgrade des Bereitstellungsmanagers von r12

Symptom:

Nachdem Upgrade des Bereitstellungsmanagers von CA Identity Manager r12 CRx zeigt das Installationsprogramm etwa folgende Meldung an:

```
Der Installationsassistent hat das Upgrade von CA Identity Manager
beendet, aber während des Upgrades traten nicht schwerwiegende
Fehler oder Warnungen auf. Details finden Sie im
Installationsprotokoll unter C:\Programme\CA\CA Identity Manager.
Warnungen/Fehler wurden in Bezug auf die folgenden Komponenten
berichtet
```

Das CA Identity Manager-Installationsprotokoll enthält den folgenden Eintrag:

```
Install, com.installshield.product.actions.Files, err,
ServiceException: (error code = -30016; message = "Der Prozess
kann nicht auf die Datei zugreifen, weil sie von einem anderen
Prozess verwendet wird."
```

Lösung:

Der Fehler tritt auf, weil das Installationsprogramm kein Verzeichnis erstellen kann, das bereits vorhanden ist. Trotzdem wurde die Installation erfolgreich abgeschlossen, und der Bereitstellungsmanager funktioniert.

Umbenennen von ACF2-, RACF- und TSS-Endpunkten vor dem Upgrade

Leerzeichen in Endpunktnamen werden nicht mehr unterstützt. Wenn Sie Endpunkte mit Leerzeichen im Namen in einer früheren Version erstellt haben, entfernen Sie diese Leerzeichen, bevor Sie das Upgrade auf 12.6 durchführen.

Ausführen des SQL Upgrade-Skripts

Wenn Sie den CA Identity Manager-Server nach dem Upgrade das erste Mal starten, wird ein Skript ausgeführt. Die Spaltengröße der Beschreibung wird in der Aufgabenpersistenz-Tabelle "runtimeStatusDetail12" auf 2000 Zeichen aktualisiert.

Wenn das Skript nicht ausgeführt werden kann, führen Sie diese Schritte durch:

1. Führen Sie eine der folgenden Aktionen aus:
   - Microsoft SQL Server: Öffnen Sie das Abfrage-Analyzer-Tool, und wählen Sie das erforderliche Skript aus.
   - Oracle: Öffnen Sie die SQL-Eingabeaufforderung für das erforderliche Skript.
2. Wählen Sie eines der folgenden Skripte aus:
   - Microsoft SQL Server: C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools\db\taskpersistence\sqlserver\archive_db_sqlserver_upgrade_to126sp2.sql
   - Oracle unter Windows: C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools\db\taskpersistence\oracle9i\archive_db_oracle_upgrade_to126sp2.sql
   - Oracle unter UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/db/taskpersistence/oracle9i/archive_db_derby_upgrade_to126sp2.sql
3. Führen Sie die Skriptdatei aus.
4. Stellen Sie sicher, dass beim Ausführen des Skripts keine Fehler angezeigt werden.

Kapitel 4: Behobene Probleme

Dieses Kapitel enthält folgende Themen:

12.6.4

Folgende Probleme wurden in CA Identity Manager 12.6.4 gelöst:

Support-Ticket	Berichtetes Problem
20957471/07	Erforderlicher Fix für CQ 170096 (IM 12.6 SP2) durchgeführt
21517465/01	Bereichsdefinition der Admin-Rolle im Suchfenster.
21536689/01	Bei der Erstellung des IM-Verzeichnisses wird ein ungültiges Kennwort beibehalten
21539813/01	Fehler beim Aktualisieren von Kontingenten und Grenzwert für LND-Konten bei auf "Manager" gesetzter ACL der E-Mail-Datei
21538682/01	In IMEs mit Token mit fehlerhaften Datumsauswahlfeldern wird in der zurückgegebenen Fehlermeldung die Schlüssel-ID anstelle des Werts des Ressourcenbündels angezeigt.
21521403/04	Das Ändern eines Dienstobjekts verursacht eine Änderung der Kategorie von "Service"
21547136/01	In Oracle-Anwendungskonten wird das Anfangsdatum von responsibilityList-Elementen in neuen Konten, die über eine Vorlage ohne festgelegtem Anfangsdatum erstellt werden, im Bereitstellungs-Manager erst sichtbar, wenn der Endpunkt wiederholt untersucht wird.
21558292/01	MEHRERE FÄLLE VON FEHLENDER 508-COMPLIANCE
20957471/09	Wenn Konten über IM mit bereits zugewiesenen Zuständigkeiten erstellt werden, werden Genehmigungen für umgekehrte Synchronisation zum Entfernen von Zuständigkeiten aus einem Oracle Apps-Konto generiert.
21551822/01	Fehlerhafte Ergebnisse bei der Objektauswahl
21567422/01	Fehlender Wert für Organisationszuordnung, in GM nach Import aus IM
20957471/11	Verhalten der Richtlinien für umgekehrte Synchronisierung für geänderte Konten fällt für Oracle Server nicht erwartungsgemäß aus
21576029/01	Beschreibung für Windows-NT-Endpunkt wird in der IM-Benutzerkonsole nicht angezeigt
21559775/01	Über die Objektauswahl in der Aufgabe "Zugriffsrolle" erstellter Rollenimport schlägt mit ungültigem XML-Zeichen (Unicode: 0x1f) fehl
21593378/01	Informationen des Managers für Live-Benachrichtigungen fehlerhaft

21590547/01	IM 12.6 SP2: AD: Leere UserPrincipalName-Attribute verursachen Synchronisierungsfehler für AD-Konten
21588715/01	Wenn eine Anzeigeregel für ein Admin-Rollen-Suchfenster definiert ist, funktioniert der Suchfilter nicht ordnungsgemäß.
21590303/01	Bei der Ausführung des neuen Massendatenlader-Client in IM r12.6 SP2 öffnet der Massendatenlader alle Aufgaben als in Bearbeitung und JVM bleibt hängen, sodass andere Anforderungen in der Warteschlange verbleiben.
21594906/01	IM 12.6 SP1: Audit-Ebene BEIDE für das Attribut wird nicht angewendet
21574514/02	IM 12.6 SP2: Aufgaben mit ausgelöstem PX im Workflow auf Ereignisebene bleiben während der Ausführung hängen
21606642/02	Langsame Leistungen mit der Aufgabe "Gruppenmitglieder ändern" bei Gruppen mit 38 000 Benutzern
21557047/01	Falsche Attributzuordnungen in Office 365 Connector?
12345678/01	Neue API für SM-Web-Agent in IM 12.6 SP4 erforderlich.
21604197/01	Import von Rollendefinitionen wird angehalten, wenn der Name von Bereitstellungsrollen "\00" enthält
21604199/01	Fehler beim Suchen von Bereitstellungsrollen bei "\" in Kombination mit Platzhalter "*".
21609415/01	Fehler beim Google-Connector aufgrund von veralteter (?) API
21626365/01	Skriptfehler beim Versuch, Seite 2 von Vorgangsdetails des Bereitstellungsmanagers anzuzeigen
21613942/01	Änderungen am Filter für Konto-Container
21419884/02	Aufnahme von Snapshots mit wenigen Filterbedingungen nimmt übermäßig viel Zeit in Anspruch
21592259/01	Kennwortfilter für Kennwortvalidierung funktioniert nicht erwartungsgemäß
21640856/01	Wenn eine durch umgekehrte Synchronisierung zum Hinzufügen einer Zuständigkeit zu einer Oracle-App generierte Genehmigung abgelehnt wird, läuft die Zuständigkeit auch dann nicht ab, wenn Sie in VST als widerrufen angezeigt wird.
21633958/01	DUPLIZIERTE BEREITSTELLUNGSROLLEN (PX)
21641737/01	Win2012: AD-Funktionalitätsebenen als Win2008R2 gemeldet
21643258/01	Wie CQ176812, jedoch für "Lesereihenfolge"
21575724/01	Regel für Benutzerbereichsdefininition für Admin-Richtlinien von Admin-Rollen führt dazu, dass Mitglieder/Administratoren einer Rolle nach einem Neustart von JBoss nicht sichtbar sind
21584724/01	Zusätzliche Protokollierung für SAP-Connector
21500603/01	CA Identity Manager- und SiteMinder-Integration schlägt fehl
21639644/01	Export von Oracle-Kontovorlagen

21657577/01	Aufgehobener Verweis auf Apache CCPP in JCS führt bei Verwendung von JavaScript in einem benutzerdefinierten CXP-Connector zu Fehlern.
21636774/01	Für Enddatum für Zuständigkeiten wird bei FND-Konten aktuelles Datum und ORA/01422 zurückgegeben: exact fetch returns more than requested number of rows ORA-06512: at "APPS_APPLSYS3.FND_USER_PKG"
21641383/01	Die Aufgabe "Benutzer aktivieren/deaktivieren" bleibt im Status "In Bearbeitung" hängen, wenn PolXpress-E-Mail konfiguriert ist.
21646678/01	Das Ant-Hilfsprogramm schlägt beim Versuch, Rollen in Token einzuteilen, fehl, wenn in Suchfenstern die Eigenschaft "Titel" hinzugefügt wird.
21657600/01	Fehler beim Import von benutzerdefinierten Feldwerten durch IM
21687010/01	Bestimmte ELM-Berichte können nicht gestartet werden.
21668810/01	Problem beim Löschen von Benutzern, die dynamischen Gruppen zugewiesen sind.
21699782/01	ARBEITSELEMENTE-LISTE - BESCHRÄNKUNG. Dieser CQ-Eintrag deckt die Arbeitsschritte ab, die erforderlich sind, um die Aufnahme von Arbeitslistenelementen in den Anmelde- bzw. Willkommensbildschirm optional zu machen.
21650405/01	Das Config Xpress-Tool lädt keine richtlinienbasierten Workflows
21539813/01	Änderungen an der Dokumentation für Behebung von Defekt PROD00176400 erforderlich.
21712883/01	IM 12.6 SP2: Active Directory-Kontoattribute für Datum/Uhrzeit werden in der IM-Benutzerkonsole nicht in der lokalen Zeitzone angezeigt
21669984/01	Wenn IDM und SM integriert sind, kann eine auf dem öffentlichen Alias mit TEWS aufgerufene private (nicht öffentliche) Aufgabe verwendet werden.
21711390/01	IM 12.6-Sicherheitsschwachstelle: Die URL zum Aufrufen einer Bildseite lässt das Definieren von contentType durch Angreifer zu, sodass im Browser eines authentifizierten Benutzers, der die URL aufruft, Code ausgeführt werden kann
21713498/01	Aufgabenstatus wird bereits während der Ausführung von Ereignissen als abgeschlissen angezeigt
21699782/01	Suche nach Initiator und Benutzer-ID zur Arbeitselemente-Liste für Benutzer hinzufügen
21704767/01	Java AXIS-Beispiel für ModifyGroupMembership.java funktioniert nicht mit 12.6 (sämtliche Service Packs). Mögliche Regression, da dies in 12.5 ordnungsgemäß funktionierte
21651991/01	Konfigurationsoptionen zum Unterdrücken von IMPS Modify_Account_Password-Benachrichtigungen zu IM hinzufügen
21730035/02	IM12.6 SP2: AD-Endpunkt: Einstellung "Benutzer muss Kennwort nach dem Zurücksetzen des Kennworts ändern" auf Endpunktregisterkarte "Konfiguration" aktualisiert keine Bereitstellungen
21730581/01	Inkonsistenz in Zertifizierer-Typ zwischen Bereitstellungsserver und LND-Endpunkt
21746621/01	Namen, die "&" enthalten, können unter OU nicht untersucht/korreliert werden

21764131/01	Das Einzelattribut Office365 für "Anmeldeinformationen sperren" wird zu eTDYN-str-multi-c/023 anstelle eines DYN-Attributs mit Einzelwert zugeordnet. Dies führt zu Fehlern beim Versuch, eine Kontosynchronisation mithilfe einer Kontovorlage des Typs "WEAK SYNC" durchzuführen.

12.6.3

Folgende Probleme wurden in CA Identity Manager 12.6.3 gelöst:

Support-Ticket	Berichtetes Problem
21088049/02	Workflow-Job antwortet nicht im "aktiven" Status.
21227662/05	Sobald ein ACF2-Endpunkt über einen angemeldeten Benutzer durchsucht wird, können Sie nicht zur Verwendung des Proxy-Admin-Benutzers wechseln.
21240169/01	"StringIndexOutOfBoundsException", wenn CA Identity Manager-Umgebung exportiert wird.
21298884/01	Zuweisen/Entfernen eines Service zu/aus einem Benutzer, der nicht in den Benutzerspeicher schreibt oder PX zu Konten auslöst.
21325322/03	Massendeaktivierungen kann nicht alle LND-Konten deaktivieren oder alle Konten zur Gruppe ohne Zugriff (Deaktiviert 0) hinzufügen
21329912/02	Kontosynchronisierung funktioniert nicht in CA Identity Manager 12.6.
21347968/01 21358148/01	Der Richtlinienserver stürzte ab, wenn eine CA Identity Manager-Zugriffsrolle zu einem Benutzer zugewiesen oder entfernt wurde.
21366658/01	Wenn Benutzer über eine Massendatenlader-Aufgabe erstellt werden, wird eine Nullzeiger-Ausnahme zurückgegeben, wenn CA SiteMinder integriert ist.
21378657/01	OOTB-Eskalations-Workflow wird vorzeitig eskaliert, wenn die Verwendung der Aufgabe "Auf globaler Richtlinie basierenden Workflow für Ereignisse konfigurieren" angegeben ist.
21378803/01	Fehler "Das vorherige Kennwort kann nicht wieder verwendet werden" tritt auf, und die Aufgabe schlägt fehl.
21385464/01	Nullzeiger-Ausnahme, wenn die Identitätsrichtlinie mit MemberRule-Gruppen und Where-Attribut-Ausdruck konfiguriert ist.
21387236/01	Beim Erstellen eines Benutzers von einer Kopie wird das Organisationsattribut nicht kopiert.
21389685/01	Anmeldezeit wird überschritten, wenn eine CA SiteMinder-Integration durchgeführt wird.
21393295/01	Fehlende Bereitstellungsrolle in der Liste der Bereitstellungsrollen des CA Identity Manager-Benutzers.
21395953/01	Policy Xpress sendet E-Mail-Schleifen.
21417960/01 21417960/03	Ändern der Bereitstellungsrolle gibt einen Nullzeiger zurück.
21424762/02	Verbotener Benutzerfehler.

Support-Ticket	Berichtetes Problem
21430655/01	Workflow-Ereignisse, die auf globaler Richtlinie basieren, werden zum Eskalationsgenehmiger verschoben.
21430868/02	Die Initialen des zweiten Vornamens können nicht entfernt werden, wenn LND-Konten umbenannt werden.
21438148/03	Die Stamm-LND-Organisation wird nicht durchsucht, und es werden keine Konten abgerufen.
21438256/01	Beispiel-Java-Skript funktioniert nicht mit der Aufgabe "Selbstregistrierung".
21438937/01	Merkwürdiges Sonderzeichen endet in der Aufgabenpersistenz "Alter Wert" und in der Überwachung.
21439600/01	Kunden finden leere Fenster, wenn sie sich mit einem abgelaufenen Kennwort anmelden.
21441213/01	Eine Verwaltungsaufgabe, die aus der CA Identity Manager-r12.5-Umgebung importiert wird, gibt den Fehler "java.lang.ClassCastException" zurück.
21447986/01	Wenn eine Policy Xpress-Richtlinie ausgelöst wird und die Anmeldung auf Norwegisch erfolgt, dann wird "java.lang.IllegalArgumentException" zurückgegeben: Ungleiche Klammern im Muster.
21450831/01	Wenn eine neue Vorlage mithilfe von Connector Xpress geöffnet wird, wird das Dialogfeld der Vorgangs-Bindung nicht angezeigt.
21468616/01	Attributlänge der Initialen des zweiten Vornamens.
21470755/01	In der mobilen Anwendung funktioniert die Managerkarte der Kontaktkarte nicht richtig.
21470794/01	In der mobilen Anwendung werden alle Fehler beim Zurücksetzen des Kennworts als komplexe Issues gemeldet, auch wenn Sie das falsche aktuelle Kennwort senden.
21473825/01	In der mobilen Anwendung von CA Identity Manager schlägt die Anmeldung fehl, nachdem ein Kennwort in der mobilen Anwendung zurückgesetzt wurde.
21475033/01	In der mobilen Anwendung von CA Identity Manager kann "Kennwort vergessen: Zurücksetzen" nur einmal verwendet werden.
21478278/01	Ein CAPTCHA-Feld im CA Identity Manager-Fenster wird nicht erneut angezeigt, wenn die Validierungsphase einige andere Felder ablehnt.
21480621/01	Bei der Installation von CA Identity Manager r12.6 SP2 auf JBoss EAP 6 konnten "iam_im_compile_jsp.*" und "build.xml" nicht installiert werden.
21481343/01	Es sind keine aktiven Slots verfügbar, da sie unbegrenzt gesperrt sind.
21486937/01	Wenn das Flag "Warten" für eine Aktionsregel in Policy Xpress für "Funktion ausführen" (nicht hauptsächlich) als Kategorie "Externer Code" und Typ "Java-Code ausführen" aktiviert ist, dann wird "JavaActionWaitEvent" durch Policy Xpress generiert, und der Status bleibt "In Bearbeitung".
21488801/01	Das Konfigurieren der Kennwortrichtlinie, die Satzzeichen benötigt, führt zu einem falschen Kennwort.

Support-Ticket	Berichtetes Problem
21497995/01	Massenvorgang gibt einen Fehler zurück, wenn ein (aus mehreren) Arbeitslistenelement der Delegation ausgewählt wird.
21520525/01	"<ETAHOME>\bin\ADSLDAPDiag.exe" schlägt fehl und gibt "Error 10054 reading data from server" zurück, wenn versucht wird, eine manuelle Verbindung zu einem Active Directory-Server 2012 herzustellen.
21522674/01	Zurücksetzungsfehler der Verbindung beim Startschritt 5.
21535004/01	Die SAP-Rolle konnte mithilfe von TEWS nicht hinzugefügt werden.
21537907/01	ConfigXpress funktioniert nicht in der CA Identity Manager r12.6 SP2-Installation.
21539251/01	Ein Fehler tritt auf, wenn eine Kopie erstellt oder die Admin-Aufgabe "Zugriffsverlauf anzeigen" geändert wird.
215544431/01	Richtlinienerstellung für globalen Workflow schlägt fehl.
21558358/01	Agentless-Exchange-Agent sucht CA CloudMinder/CAFT
21568224/01	"ConfigXpress.air" funktioniert nicht - Bei der CA Identity Manager r12.6 SP2-Installation wird ein Fehler zurückgegeben.
21572374/01	In der mobilen Anwendung von CA Identity Manager funktioniert die schnelle Genehmigung nicht.
21585328/01	"ConfigXpress.air" kann nicht auf CA Identity Manager r12.6 SP2 installiert werden.

12.6.2

Folgende Probleme wurden in CA Identity Manager 12.6.2 gelöst:

Support-Ticket	Berichtetes Problem
21198613/01	Das von PX festgelegte Kennwort wird nicht mit dem globalen Benutzer und den Konten synchronisiert.
21230281/01	Logical-Attribute-Handler können nicht in die Management-Konsole importiert werden.
21263275/01	Probleme mit Arcot-Kennwortrichtlinie.
21269108/02	Probleme mit der Installation des Agenten für die Kennwortsynchronisierung von CA Identity Manager r12.6.
21264877/01	Admin-DN wird an die externe URL angehängt.
21275958/01	Nullzeiger-Ausnahme beim Erfassen eines SAP-Endpunkts.
21272983/01	Fehler beim Lesen des CA Access Control-Endpunkts mit mehreren definierten Richtlinienmodell-Datenbanken (PMDBs).

Support-Ticket	Berichtetes Problem
21173122/01	Importierte "rolesDef" wird nicht angezeigt.
21270763/01	Ein Fehler tritt auf, wenn ein Bereitstellungsverzeichnis mithilfe des Assistenten erstellt wird.
21280342/01	"DoSynchUserRoles" aktiviert nicht die Kontrollkästchen für "Fehlende Konten hinzufügen" und "Extra-Konten entfernen" für den CA Identity Manager Task Execution Web Service (TEWS) und die Web Services Description Language (WSDL).
21285651/01	Kompatibilität der Aufgabe "Konten mit Kontovorlage synchronisieren" mit TEWS.
21295778/01	Der Fehler "Error instantiating Policy Xpress plugin" tritt auf, wenn versucht wird, Policy Xpress-Richtlinien zu erstellen oder zu ändern.
21304316/01	Leistungsprobleme, wenn Gruppen mithilfe der Benutzeraufgaben "Erstellen" oder "Ändern" zu einem Benutzer hinzugefügt werden.
21304316/02	Leistungsprobleme, wenn Gruppen mithilfe der Schaltfläche "Gruppen hinzufügen" auf der Aufgabe "Benutzer ändern" zu einem Benutzer hinzugefügt werden.
21306987/01	Ein "NoClassDefFoundError"-Fehler tritt auf, wenn "highavailability.bat" ausgeführt wird.
21307126/01	RSA Secure ID 7 - Es kann kein Endpunkt erfasst werden, da Probleme mit dem Skript für die Erstellung eines Open Services Gateway Initiative-Bundle (OSGi) vorhanden sind.
21315277/04	C++ Connector Server stürzt ab, wenn nach verschobenen oder nach umbenannten Active Directory-Benutzerkonten (AD) gesucht wird.
21319140/01	Die importierte SQL-basierte "dir.xml"-Daten sind großgeschrieben.
21322022/01	CA Identity Manager-Anmeldungen werden mit der Zeit langsamer.
21325322/01	"Session closed due to communications failure" auf LND, wenn Konten geändert werden.
21331632/01	Warnmeldung, wenn ein Service widerrufen wird, der den Benutzernamensparameter nicht enthält.
21335464/01	Skriptfehler im Bereitstellungsmanager, wenn ein Vorgang angezeigt wird, der mehrere Seiten umfasst.
21351855/01	CA Identity Manager kann keine Umgebung erstellen, wenn keine Bereitstellung und nur Systemmanagerrolle ausgewählt wurden.
21361599/01 21383034/01	Folgender Fehler wird angezeigt, wenn die Aufgabe "Benutzer ändern" verwendet wird: Aufgabe mit schwerem Fehler: "SynchronizeAttributesWithAccountEvent" konnte nicht ausgeführt werden: FEHLERMELDUNG: For input string
21393461/01	Ausnahme beim Aktualisieren von "Benutzer aktivieren/deaktivieren" oder eines anderen Benutzerattributs.

12.6.1

Die folgenden Probleme wurden in CA Identity Manager 12.6.1 gelöst:

Support-Ticket	Berichtetes Problem
20576709/02	Unterstützung der Freigabe des gemeinsamen BusinessObjects Report Server sowohl für CA Identity Manager als auch SiteMinder erforderlich
20576725/02	Unterstützung von BusinessObjects Report Server in einer Hochverfügbarkeitskonfiguration erforderlich
20583665/02	Unterstützung für BusinessObjects Report Server XI 3.1 SP5 (CABI 3.3) erforderlich
20774861/02	Fehler beim Einfügen von Daten sekundärer Objekte in Policy Xpress
20777137/02	Es wurden Verbesserungen am Richtlinien-basierten Workflow vorgenommen, bei dem sekundäre Objekte (Benutzerobjekte) abgerufen werden, die von primären Objekten benötigt werden.
20888199/01	DN-Namenskonvention für Kontovorlagen für TEWS nicht dokumentiert
21073146/01	"Synchronisieren von Konten mit Kontovorlage" synchronisiert nicht
21086870/01	Eigenständiges JCS-Installationsprogramm verlangt nicht nach Eingabe des FIPS-Schlüssels, was zu Problemen bei der Verschlüsselung führt
21108813/01	CA Identity Manager 12.6 stellt nicht die erwarteten Rollendefinitionen bereit
21111634/01	JCS-Endpunktprotokolle werden nicht erstellt
21131768/01	Probleme mit dem Attribut für globalen Richtlinien-basierten Workflow (sekundärer Objekttyp fehlt für Ereignisdefinitionen)
21135604/01	Keine Anzeige der Aufgabe "Logical-Attribute-Handler" wegen NullPointer-Fehler
21136454/01	SQL-Injektions-Sicherheitsschwachstellen wurden in dieser Version beseitigt
21136456/01	Sicherheitsschwachstellen
21136499/01	Auswahlfelddaten funktionieren nicht bei einem Profil-Fenster, das in CA Identity Manager 12.6 an einen Dienst angehängt ist
21137701/01	Ausnahme "PxEnvironmentException" wird empfangen, wenn Policy Xpress-Richtlinien externen Java-Code aufrufen
21140501-1	Unterstützung für Cloud-Bereitstellungen (Mandantenverwaltung)
21146621/01	Globale Attributvalidierung in "directory.xml"
21156269/01	Unterschiede zwischen den vom Installationsprogramm und den individuellen Datenbankskripten im Toolsordner generierten DB-Schemen
21156269/01	Mehr Skripte für manuelle Datenbankerstellung benötigt

Support-Ticket	Berichtetes Problem
21162602/01	Benutzerdefinierte Korrelation für TSS funktioniert nicht unter Unix
21170706/01	Ergebnisse der Aufgabe "Gesendet anzeigen" sind falsch sortiert, wenn Gebietsschema auf Dänisch eingestellt ist
21175201/01	Von eingehender Benachrichtigung initiierte Kontosynchronisierung wird nicht ausgeführt, wenn Bereitstellungsrollen mithilfe von Policy Xpress-Richtlinien zugewiesen werden
21181592/01	Fehler beim Laden von CA Identity Manager r12.6 wegen ungültigem Klassenpfad
21183366/01	Falscher Benutzername bei Verwendung von Datenquellen
21187385/01	Wiederholte CA Identity Manager-Abstürze
21188814/01	SiteMinder r12 SP3 CR11-Richtlinienserver stürzt ab, während auf CA Identity Manager-Richtlinie zugegriffen wird
21190699/01	Abrufen sekundärer Objektinformationen durch Policy Xpress schlägt entweder bei Ereignis- oder Aufgaben-basierten Richtlinien fehl. Der ursprüngliche Attributwert wird auch zurückgegeben, sogar wenn Policy Xpress diesen nach Abschluss der Aufgabe entfernt.
21190873/01	508 Compliance-Problem: QuickInfos von Kontrollkästchen haben keine Bedeutung.
21193837/01	Erstellen und Löschen von verwalteten Objekten
21194712-1	Policy Xpress mit Iterator wird unterbrochen, wenn eine ausgelöste Zugriffsrollenzuweisung vom Workflow abgelehnt wird
21200396/01	508 Compliance-Problem: Link-Probleme bei "Zum Hauptinhalt wechseln"
21200412/01	508 Compliance-Problem: Warn- und Fehlermeldungen werden von Unterstützungssoftware für deaktivierte Benutzer nicht richtig gelesen.
21213029-1	Die im JSession-Zwischenspeicher gespeicherten Kennwortdienstvariablen werden nicht gelöscht (beim Abmelden), und nachfolgende Anfragen werden zur "pws.fcc"-Seite umgeleitet

Kapitel 5: Dokumentation

Die Dateinamen der CA Identity Manager-Handbücher sind:

Handbuchname	Dateiname
Versionshinweise	im_release_deu.pdf
Implementierungshandbuch	im_impl_deu.pdf
Installationshandbuch für WebLogic	im_install_weblogic_deu.pdf
Installationshandbuch für WebSphere	im_install_websphere_deu.pdf
Installationshandbuch für JBoss	im_install_jboss_deu.pdf
Aktualisierungshandbuch	im_upgrade_deu.pdf
Konfigurationshandbuch	im_config_deu.pdf
Administrationshandbuch	im_admin_deu.pdf
Benutzerkonsolendesign-Handbuch	im_uc_design_deu.pdf
Programmierhandbuch für Java	im_dev_deu.pdf
Provisionierungs-Referenzhandbuch	im_provisioning_reference_deu.pdf
Connectors-Handbuch	im_connectors_deu.pdf
Handbuch für Connector Xpress	im_connector_xpress_deu.pdf
Implementierungshandbuch für Java Connector Server	im_jcs_impl_deu.pdf
Programmierhandbuch für Java Connector Server	im_jcsProg_deu.pdf
Glossar	im_glossary.pdf
Bookshelf	im_bookshelf_deu.zip

Dieses Kapitel enthält folgende Themen:

Bookshelf

Das Bookshelf ermöglicht den Zugriff auf die gesamte CA Identity Manager Dokumentation über eine einzige Oberfläche. Folgende Funktionen sind enthalten:

- Erweiterbare Inhaltsangabe für alle Handbücher im HTML-Format
- Volltextsuche über alle Handbücher mit bewerteten Suchergebnissen und im Inhalt hervorgehobenen Suchbegriffen
- Klickelemente ("Brotkrümel"), die zu übergeordneten Themen führen
- Ein einziger HTML-Index für Themen in allen Handbüchern
- Links zu PDF-Versionen der Handbücher zum Drucken

So verwenden Sie den Bookshelf:

1. Laden Sie den Bookshelf von der Support-Website von CA herunter.
2. Entpacken Sie den Inhalt der komprimierten Bookshelf-Datei (.zip).

   Hinweis: Um eine bessere Leistung zu erhalten, sollten Sie, wenn Sie das Bookshelf auf einem Remote-System installieren, den Zugriff auf das Bookshelf über einen Webserver zulassen.
3. Zeigen Sie das Bookshelf wie folgt an:
   - Wenn sich das Bookshelf auf dem lokalen System befindet, und Sie Internet Explorer verwenden, öffnen Sie die Datei Bookshelf.hta.
   - Wenn sich das Bookshelf auf einem Remote-System befindet, oder wenn Sie Mozilla Firefox verwenden, öffnen Sie die Datei Bookshelf.html.

     Hinweis: Um eine bessere Leistung zu erhalten, sollten Sie, wenn Sie das Bookshelf auf einem Remote-System installieren, den Zugriff auf das Bookshelf über einen Webserver zulassen.

Zum Anzeigen des Bookshelfs ist Internet Explorer 7 oder 8 bzw. Mozilla Firefox 2 oder 3 erforderlich. Für die Links auf PDF-Handbücher ist Adobe Reader 7 oder höher erforderlich. Sie können Adobe Reader unter www.adobe.com herunterladen.

Bekannte Probleme

Alle bekannten Probleme mit Bezug zu CA Identity Manager sind auf der Website des CA Support dokumentiert.

Versionshinweise für CA Identity Manager- und CA Identity Governance-Integration

Alle auf die Integration zwischen CA Identity Manager und CA Identity Governance bezogenen Versionshinweise befinden sich in den *Versionshinweisen für CA Identity Governance*. Sie können auf das CA Identity Governance-Bookshelf über CA Support zugreifen.

Anhang A: Barrierefreiheitsfunktionen

CA Technologies möchte sicherstellen, dass alle Kunden unabhängig von ihren Fähigkeiten die Produkte und die unterstützende Dokumentation erfolgreich einsetzen können, um damit zentrale Geschäftsaufgaben durchführen zu können. Dieser Abschnitt beschreibt die Eingabehilfen, die Teil von CA Identity Manager sind.

508 Compliance

CA Identity Manager ist konform mit Abschnitt 508 des US Rehabilitation Avt und den Web Content Accessibility Guidelines (WCAG2.0) auf AA-Ebene. Das Thema Produktverbesserungen (siehe Seite 67) bietet weitere Details. Sie können auch Ihren Account Manager nach einer Kopie des Voluntary Product Accessibility Template (VPAT) von CA Technology fragen.

Produktverbesserungen

CA Identity Manager bietet Zugangsverbesserungen in den folgenden Bereichen:

- Anzeige
- Klang
- Tastatur
- Maus

Hinweis: Die folgenden Informationen beziehen sich auf Anwendungen unter Windows und Macintosh. Auf vielen Hostbetriebssystemen werden Java-Anwendungen ausgeführt, für die dort bereits Eingabehilfen verfügbar sind. Damit diese vorhandenen Eingabehilfen Zugriff auf Programme haben, die in JPL geschrieben sind, benötigen sie ein Bridge zwischen sich in ihren systemeigenen Umgebungen und der Java-Zugriffsunterstützung, die über die Java Virtual Machine (oder Java VM) verfügbar ist. Das eine Ende dieser Bridge ist in der Java VM und das andere auf der systemeigenen Plattform. So ist sie bei jeder Plattform unterschiedlich. Sun entwickelt gegenwärtig sowohl die JPL- als auch die Win32-Seite dieser Bridge.

Anzeige

Um die Sichtbarkeit auf Ihrer Computer-Anzeige zu vergrößern, können Sie die folgenden Optionen einstellen:

Schriftart, Farbe und Größe von Elementen

Ermöglicht die Auswahl der die Schriftartfarbe, der Größe und anderer visueller Kombinationen.

Bildschirmauflösung

Ermöglicht das Ändern der Pixelanzahl, um Objekte auf dem Bildschirm zu vergrößern.

Breite und Blinkrate des Cursors

Sorgt dafür, dass der Cursor leichter zu finden ist oder sein Blinken minimiert wird.

Symbolgröße

Ermöglicht das Vergrößern von Symbolen für bessere Sichtbarkeit oder das Verkleinern für mehr Bildschirmfläche.

Schemen für hohen Kontrast

Ermöglicht die Auswahl von Farbkombinationen, die besser zu sehen sind.

Klang

Verwenden Sie Klang als Alternative zur visuellen Darstellung oder um Computer-Klänge leichter hörbar oder unterscheidbar zu machen. Folgende Optionen können dazu angepasst werden:

Lautstärke

Ermöglicht das Erhöhen oder Verringern der Lautstärke des Computer-Klangs.

Text-zu-Sprache

Ermöglicht das Hören von Befehlsoptionen und Text durch laute Vorlesen.

Warnungen

Ermöglicht die Anzeige visueller Warnungen.

Hinweise

Gibt Ihnen akustische oder visuelle Zeichen, wenn Zugriffsfunktionen ein- oder ausgeschaltet werden.

Schemen

Ermöglicht die Zuordnung von Computer-Klängen zu bestimmten Systemereignissen.

Bezeichnungen

Ermöglicht die Anzeige von Bezeichnungen für Sprache und Klänge.

Hinweis: Wenn Sie ein Sprachausgabeprogramm verwenden, empfehlen wir, dass Sie die aktuelle Version des Tools für eine bessere Interpretation installieren.

Tastatur

Sie können die folgenden Tastaturanpassungen vornehmen:

Wiederholrate

Ermöglicht es einzustellen, wie schnell sich ein Zeichen wiederholt, wenn eine Taste gedrückt bleibt.

Töne

Ermöglicht die Ausgabe von Tönen, wenn bestimmte Tasten gedrückt werden.

Feststelltasten

Ermöglicht jenen, die mit nur einer Hand oder einem Finger tippen, alternative Tastaturlayouts auswählen.

Überspringen-Link

Ermöglicht die Nutzung des Links "Zum Hauptinhalt wechseln" für eine schnelle Navigation zum Hauptinhalt.

Maus

Sie können die folgenden Optionen verwenden, um Ihre Maus schneller zu machen und die Handhabung zu verbessern:

Klickgeschwindigkeit

Ermöglicht die Einstellung, wie schnell auf die Maustaste geklickt werden soll, um eine Auswahl zu machen.

Klicksperre

Ermöglicht das Hervorheben oder Ziehen, ohne die Maustaste gedrückt zu halten.

Umgekehrte Aktion

Ermöglicht das Umkehren der Aktionen, die über die linke und rechte Maustaste gesteuert werden.

Blinkrate

Ermöglicht die Einstellung, wie schnell der Cursor blinkt oder ob er überhaupt blinkt.

Zeigeroptionen

Ermöglicht Folgendes:

- Ausblenden des Zeigers während der Eingabe
- Anzeigen der Position des Zeigers
- Einstellen der Geschwindigkeit, mit der der Zeiger auf dem Bildschirm bewegt wird
- Auswählen der Größe und Farbe des Zeigers für bessere Sichtbarkeit
- Bewegen des Zeigers zu einer Standardposition in einem Dialogfeld

Ausnahmen bei Mozilla Firefox

Wir empfehlen, dass Tastaturbenutzer und JAWS-Benutzer aus folgenden Gründen den Internet Explorer 8 verwenden:

- In Firefox erhalten Dialogfelder den In/Out-Fokus nicht.
- In Firefox wird der Link "Zum Hauptinhalt wechseln" von der Sprachausgabe nicht immer zuerst vorgelesen.

Tastenkombinationen

Die folgende Tabelle listet die Tastenkombinationen auf, die CA Identity Manager unterstützt:

Tastatur	Beschreibung
Ctrl+X	Ausschneiden

Tastatur	Beschreibung
Ctrl+C	Kopieren
Ctrl+K	Weitersuchen
Ctrl+F	Suchen und Ersetzen
Ctrl+V	Einfügen
Ctrl+S	Speichern
Ctrl+Shift+S	Alles speichern
Ctrl+D	Löschen der Zeile
Ctrl+Nach rechts	Nächstes Wort
Ctrl+Nach unten	Zeile nach unten scrollen
Ende	Ende der Zeile

CA Technologies-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA Technologies:

- CA CloudMinder™ Identity Management
- CA Directory (NeteAuto-Verzeichnis)
- CA Identity Manager ™
- CA Identity Governance (früher CA GovernanceMinder)
- CA SiteMinder®
- CA Berichte zu Benutzeraktivitäten
- CA AuthMinder ™

Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Kapitel 6: Bekannte Probleme

Dieses Kapitel enthält folgende Themen:

Allgemein

Folgende Probleme sind allgemein bekannt in CA Identity Manager r12.5 SP1.

Formatierungsprobleme beim Wechseln zwischen HTML- und Textansichten

Symptom:

Wenn Sie eine E-Mail im HTML-Editor erstellen oder ändern und zwischen HTML- und Textansicht wechseln, können Formatierungsprobleme wie Änderungen an Tabellenfarben oder Verschiebungen von Tabellen auftreten. Diese Probleme wurden in Internet Explorer 9 unter Windows 7 beobachtet.

Lösung:

Verwenden Sie andere unterstützte Browser. Weitere Informationen zu unterstützten Browsern finden Sie in der Plattformunterstützungs-Matrix von CA Identity Manager r12.6 SP4.

Beschränkungen von Configuration Xpress bei der Migration von Objekten zwischen Umgebungen

Symptom

Bestimmte Objekte wie z. B. Workflow-Zuordnungen können nicht mit Config Xpress in eine andere Umgebung hochgestuft werden.

Lösung:

1. Melden Sie sich bei der Benutzerkonsole an, und navigieren Sie "Systeme", "Auf globaler Richtlinie basierenden Workflow für Ereignisse konfigurieren".

   Hinweis: Sie können auch zur Management-Konsole, "Erweiterte Einstellungen", "Workflow" gehen.

2. Ordnen Sie ein Ereignis zu einem Workflow, bei dem es sich nicht um eine Vorlage handelt, zu.

   Hinweis: Dieses Ereignis sollte nicht aus der OOTB-Zuordnungsliste stammen.

   Beispiel: ModifyAccessRoleMembershipApproveProcess zu AssignAccessRoleEvent zugeordnet.

3. Exportieren Sie die Datei Environmentsetting.xml über die Einstellung "Erweitert" der Management-Konsole.

4. Löschen Sie die in Schritt 2 neu hinzugefügte Zuordnung.

5. Importieren Sie die Datei Environmentsetting.xml aus Schritt 3.

   Die in Schritt 2 erstellte Zuordnung sollte nach dem Import vorhanden sein.

Fehler beim Kennwortzurücksetzungsverhalten "QnA" bei Verwendung der Standardeinstellung für "Konfiguration für Fragen und Antworten"

Das Kennwortzurücksetzungsverhalten "QnA" schlägt bei Verwendung der Standardeinstellung für "Konfiguration für Fragen und Antworten" im Umgebungsadministrator von IdentityMinder-Aufgaben fehl.

Symptom

Wenn Sie als Kennwortzurücksetzungsverhalten "QnA" festlegen und die Standardeinstellung für "Konfiguration für Fragen und Antworten" verwenden, schlägt die Kennwortzurücksetzung mit folgender Fehlermeldung fehl:

"ERROR [im.webservices.QuestionAndAnswerResource] (http-/0.0.0.0:8443-1) Failed to process get user credential questions. Message:java.lang.NullPointerException in the server log file"

Lösung:

Führen Sie folgende Schritte aus, damit Kennwortzurücksetzungen mit Kennwortzurücksetzungsverhalten "QnA" ordnungsgemäß funktionieren:

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Identity Minder als SuperAdmin an.
2. Navigieren Sie zu "Aufgaben", "Umgebungsadministrator", und wählen Sie "Konfiguration für Fragen und Antworten" aus.
3. Klicken Sie auf die Schaltfläche "Senden".

   Hinweis: Die Standardwerte für die Option "Aktivieren" und für "Anzahl der Authentifizierungsfragen" werden ebenfalls erst nach der Durchführung dieses Schritts angewendet.

Kennwortzurücksetzung schlägt nach Upgrade von IdentityMinder 12.6 SP2 oder SP3 zu SP4 fehl

Symptom:

Nach einem Upgrade von CA IdentityMinder r12.6 SP2 oder SP3 auf 12.6 SP4 funktioniert "Kennwort zurücksetzen" nicht, da die Option "Kennwortzurücksetzungsverhalten" in "Mobile Konfiguration" nicht festgelegt ist.

Lösung:

Führen Sie die folgenden Schritte aus, um "Kennwortzurücksetzungsverhalten" manuell zu aktivieren.

1. Melden Sie sich bei Identity Minder als SuperAdmin an.
2. Navigieren Sie zu "Aufgaben", "System", "Mobile Konfiguration", und klicken Sie auf "Mobile Konfiguration ändern".
3. Wählen Sie die mobile Konfiguration aus, und navigieren Sie zur Registerkarte "Funktionen".
4. Wählen Sie manuell eine der verfügbaren Optionen für "Kennwortzurücksetzungsverhalten" aus.
5. Senden Sie die Aufgabe.

Fehler, wenn viele Services dargestellt werden

Symptom:

Wenn viele Services von CA Identity Manager angezeigt werden, generiert Axis2 eine große Stub-Klasse, die die JVM-Übersetzungsregel verletzt, und es wird folgender Fehler zurückgegeben:

```
error: code too large for try statement
```

Lösung:

Wenn Sie einen solchen Übersetzungsfehler erhalten, führen Sie folgende Schritte aus:

1. Öffnen Sie die generierte Stub-Klassendatei aus folgendem Beispielverzeichnis:

   ```
   <samples_dir>\wsdl2java\src\tew6\wsdl
   ```

   Axis2 generiert die Stub-Klasse im folgenden Format:

   ```
   <Service_name>Stub.java
   ```

   Hinweis: Rufen Sie den Servicenamen aus WSDL ab.

2. Teilen Sie in der Stub-Klassendatei die Methoden "fromOM" und "populateFaults". Folgendes Skript ist ein Beispiel für die Methode "fromOM" aus der Stub-Klassendatei:

   ```
   public org.apache.xmlbeans.Xmlobject fromOM (
   org.apache.axiom.om.OMElement param,
   java.lang.Class type,
   java.util.Map extraNamespaces) throws
   org.apache.axis2.AxisFault {
   try {
   .......
   .......
   .......
   }catch (java.lang.Exception e) {
   throw org.apache.axis2.AxisFault.makeFault(e);
   }
   return null;
   }
   ```

3. Teilen Sie das Methodenskript in zwei Hälften, und benennen Sie die andere Hälfte zum Beispiel "fromOMExtended".

4. Rufen Sie die neu erstellte Methode von der Methode "fromOM" ab. Folgendes Skript ist ein Beispiel für die geänderte Methode "fromOM":

   ```
   public org.apache.xmlbeans.Xmlobject fromOM (
   org.apache.axiom.om.OMElement param,
   java.lang.Class type,
   java.util.Map extraNamespaces) throws
   org.apache.axis2.AxisFault {
   try {
   .......
   .......
   ```

```
.......
}catch (java.lang.Exception e) {
throw org.apache.axis2.AxisFault.makeFault(e);
}
//invoking the new method
return this. fromOMExtended(param, type, extraNamespaces);
}
```

5. Wiederholen Sie die Schritte 3 und 4 für die Methode "populateFaults".

6. Speichern Sie die Änderungen, und führen Sie folgenden Befehl vom Speicherort des Beispielverzeichnisses für die Kompilierung der Änderungen aus:

   ```
   sample_dir_location> ant -Dnowsdlgen=true
   ```

   Die Kompilierung gibt keinen Fehler zurück.

Kennwort in Klartext gespeichert

Symptom:

Das Kennwort für den sicheren Bootstrap-Benutzer der Management-Konsole wird in Klartext gespeichert.

Lösung:

Verwenden Sie das Kennwort-Tool, das im Installationspaket enthalten ist, um das Kennwort mit der Option "–JSAFE" zu verschlüsseln. Weitere Informationen über das Kennwort-Tool finden Sie im Konfigurationshandbuch.

Zu viele Genehmiger in der Liste der Genehmiger

Symptom:

Zu viele Genehmiger in der Liste der Genehmiger gibt folgenden Fehler zurück:

```
ORA-12899: Value too large for column error
```

Die Aufgabe schlägt fehl, und der Workflow wird nicht fortgesetzt.

Lösung:

Führen Sie folgende SQL-Befehle in der Oracle-Datenbank aus, wo die Berichtsdatenbank (Objektspeicher) gespeichert ist.

```
ALTER TABLE WP_ACT_DATA  MODIFY (VAR_VALUE NVARCHAR2(2000));
ALTER TABLE WP_ACTI_DATA   MODIFY (VAR_VALUE NVARCHAR2(2000));
ALTER TABLE WP_PROC_DATA   MODIFY (VAR_VALUE NVARCHAR2(2000));
ALTER TABLE WP_PROCI_DATA   MODIFY (VAR_VALUE NVARCHAR2(2000));
```

Über Credential Provider in Windows 2012- und Windows 8-Plattformen kann keine Verbindung zu den Seiten "Kennwort vergessen" und "Konten entsperren" hergestellt werden

Windows 2012 funktioniert aufgrund von Windows 8 nicht mit Credential Provider, da Microsoft die Schnittstelle geändert hat

404 nach der Bestätigung zum Zurücksetzen des Kennworts, da "pws.fcc" fehlt

Symptom:

Es wird eine öffentliche IM-Aufgabe mit dem Namen "CPSChangeMyPassword" verwendet, in der der Benutzer sein altes und sein neues Kennwort und die Bestätigung eingibt. Sobald Sie auf "Senden" klicken und dann auf der nachfolgenden IM-Bestätigungsseite mit "OK" bestätigen, dann wird die Fehlermeldung "404 File Cannot Be Found" angezeigt.

Lösung:

Der SiteMinder 12.5 IIS-Web-Agent enthält nicht die Datei "PWS.fcc" in den virtuellen IIS-Verzeichnisformularen. Kopieren Sie die Datei "PWS.fcc" aus der früheren CA Identity Manager-Version.

Hinzufügen von benutzerdefinierten E-Mail-Vorlagen für Serviceobjekte

Um bei Serviceobjekten E-Mail-Benachrichtigungen und den Ablauf des Services zu erhalten, müssen Sie eine benutzerdefinierte E-Mail-Vorlage erstellen.

Gehen Sie wie folgt vor:

1. Wechseln Sie in das folgende Verzeichnis: `%JBOSS_HOME%\server\default\deploy\iam_im.ear\custom\emailTemplates\default.`
2. Erstellen Sie eine benutzerdefinierte E-Mail-Vorlage mit dem Namen "AddServiceToUserEvent.tmpl" im folgenden Ordner: `iam_im.ear\custom\emailTemplates\default\service_status_folder`
3. Wenn der Service abgeschlossen oder ausstehend ist, ändern Sie den Status entsprechend in Zeile 38.
4. Überprüfen Sie, ob die Benachrichtigung und der Ablauf in der generierten E-Mail aktualisiert wurden.

Fehler bei der Installation von CA Identity Manager mit UTF-8-Zeichen im Installationspfad oder in den Datenbankdetails in allen nicht-englischen Sprachen

Symptom:

Wenn Sie versuchen, die CA Identity Manager 12.6 SP3-Installation mit UTF-8-Zeichen im Installationspfad oder in den Datenbankdetails (DB-Name, DB-Benutzername und DB-Kennwort) in nicht-englischer Sprache auszuführen, dann tritt folgender Fehler in den Installationsprotokollen auf, und die Installation schlägt fehl:

```
C:\Users\Administrator\AppData\Local\Temp\1\598343.tmp\installFrag
ments\dataSource.xml:329: Invalid byte 2 of 4-byte UTF-8 sequence.
```

Lösung:

Verwenden Sie Nicht-UTF-8-Zeichen (Englischer Text) im Installationspfad oder in den Datenbankdetails (DB-Name, DB-Benutzername und DB-Kennwort), und fahren Sie mit der Installation auf den folgenden unterstützten systemfremden, nicht-englischen Sprachen wie z. B. Französisch, Italienisch, Deutsch, Spanisch, Japanisch, brasilianisches Portugiesisch, vereinfachtes Chinesisch, Koreanisch, Finnisch, Norwegisch, Schwedisch, Dänisch und Polnisch fort.

Verbindungsfehler nach einem Upgrade des CA Identity Minder-Servers

Symptom:

Es tritt ein Verbindungsfehler auf, wenn ein Zugriff von CA Identity Manager auf CA Identity Governance erfolgt, nachdem ein Upgrade einer vorhandenen Installation durchgeführt wurde.

Lösung:

Nach einem CA Identity Manager-Server-Upgrade sind weitere Konfigurationen erforderlich.

Gehen Sie wie folgt vor:

1. Gehen Sie in der CA Identity Manager-Benutzerkonsole zu "System", "Webservices", "Webservices-Konfiguration löschen", "Suchen".
2. Löschen Sie die IMRCM-Konfiguration.
3. Melden Sie sich beim Webportal von CA Identity Governance an.
4. Gehen Sie zu "Administration", "Universum", und wählen Sie das Universum aus, das für die Integration mit CA Identity Manager konfiguriert wurde.
5. Gehen Sie auf die Registerkarte "Konnektivität", und wählen Sie den CA Identity Manager-Connector aus.

Klicken Sie auf "Test", und bestätigen Sie, dass die Verbindung erfolgreich ist.

Warnmeldung, wenn ein OOTB-Snapshot-DDL-Skript ausgeführt wird

Symptom:

Folgendes SQL-Skript erzeugt einen ungültigen Index, wenn es auf einer Microsoft SQL-Datenbank ausgeführt wird:

`IdentityManager/IAM_Suite/IdentityManager/tools/imrexport/db/SqlServer/ims_mssql_report.sql`

Das Skript wird mit folgender Warnmeldung zurückgegeben:

Warnung! Die maximale Schlüssellänge ist 900 Byte. Der Index "imruser6_index_3" hat eine maximale Länge von 1260 Byte. Bei einigen Kombinationen aus großen Werten wird der Einfügungs-/Aktualisierungsvorgang fehlschlagen.

Lösung:

Gehen Sie wie folgt vor:

1. Verwenden Sie folgenden Code, um eine gespeicherte Prozedur zu erstellen:
   ```
   CREATE PROCEDURE sp_imruser6_index_3_exists
   AS
   BEGIN
   DECLARE @MAX_LEN integer
   DECLARE @sql_cmd nvarchar(255)
   DECLARE @stmt nvarchar(255)
       SET @MAX_LEN = (SELECT SUM(max_length)AS TotalIndexKeySize
   FROM sys.columns WHERE name IN (N'imr_userdn', N'imr_reportid')
   AND object_id = OBJECT_ID(N'imruser6'))
            IF EXISTS (SELECT name FROM sysindexes WHERE name =
   'imruser6_index_3') DROP INDEX imruser6_index_3 on imruser6
       IF (@MAX_LEN > 900)
           CREATE INDEX imruser6_index_3 ON imruser6
   (imr_reportid) INCLUDE(imr_userdn)
       ELSE
           CREATE INDEX imruser6_index_3 ON imruser6
   (imr_reportid, imr_userdn)
   END
   GO
   ```
   Die gespeicherte Prozedur ist nun erstellt.
2. Verwenden Sie folgenden Befehl, um die gespeicherte Prozedur auszuführen:
   ```
   EXEC sp_imruser6_index_3_exists
   ```

Nachdem Sie die gespeicherte Prozedur erfolgreich ausgeführt haben, wird die Spalte "imr_userdn" unter "imruser6_index_3" zur eingeschlossenen Spalte.

Nicht-kontextbezogene Hilfe für mobile App

Symptom:

Wenn ein Benutzer beim Ausführen von Aufgaben der mobilen App auf das Hilfesymbol klickt, dann wird nicht zugehörige Hilfe angezeigt.

Lösung:

Suchen Sie die Hilfe der mobilen App im Inhaltsverzeichnis oder indem Sie die Hilfe suchen.

Bereitstellungsverzeichnis lässt sich nicht über die Management-Konsole erstellen

Beim Erstellen eines Bereitstellungsverzeichnisses über die Management-Konsole darf der Domänenname des Bereitstellungsservers keine fremdsprachigen Zeichen enthalten. Folgende Fehlermeldung wird angezeigt:

"could not connect to the LDAP server machinename:20389 with userDN etGlobalUserName=admin,eTGlobalUserContainerName:GlobalUsers,eTNamespacename=CommonObjects,dc=foreignChars, dc=eta and specified password."

AttributeLevelEncryption für Benutzerkennwörter

Wenn Sie die "AttributeLevelEncryption"-Datenklassifizierung für Attribute in der Verzeichniskonfigurationsdatei ("directory.xml") angeben, verschlüsselt CA Identity Manager den Attributwert im Benutzerspeicher. In der Benutzerkonsole wird der Wert in Klartext angezeigt.

Die folgende Attributbeschreibung zeigt die "AttributeLevelEncryption"-Datenklassifizierung:

```
<ImsManagedObjectAttr physicalname="title" description="Title"
displayname="Title" valuetype="String" maxlength="0"
searchable="false">

<DataClassification name="AttributeLevelEncrypt"/>

</ImsManagedObjectAttr>
```

In Umgebungen mit der folgenden Konfiguration werden bei Verschlüsselung der Kennwörter auf Attributebene Benutzer daran gehindert sich anzumelden:

- CA Identity Manager-Integration von CA SiteMinder und
- Benutzerspeicher ist eine relationale Datenbank

In dieser Version wurde die "AttributeLevelEncryption"-Datenklassifizierung aus dem Kennwortattribut der folgenden Verzeichniskonfigurationsdateien ("directory.xml") entfernt:

- DirectoryTemplates/RelationalDatabase.xml
- fwSampleRDB.xml
- Samples/NeteAutoRDB/NoOrganization.xml
- Samples/NeteAutoRDB/Organization.xml

Diese Dateien befinden sich im Verzeichnis *admin_tools*.

Hinweis: Weitere Informationen zur Verwaltung vertraulicher Attribute finden Sie im *Konfigurationshandbuch*.

Spezifizieren von LDAP-DN bei Verwendung von TEWS

Symptom:

Bei der Verwendung von TEWS zum Aufrufen der Aufgabe "CreateOracleServerAccountTemplate" können Sie folgende Fehlermeldung zurückerhalten:

```
Error Message: <code>500</code>

<description>Failed to execute CreateOracleServerAccountTemplate. ERROR

MESSAGE: com.ca.iam.model.IAMParseException: Not a valid IAM handle:

'UHGUSERS' ProcessStep::Unknown TabName: null ERRORLEVEL::Fatal</description>
```

Das Problem besteht darin, dass TEWS nicht denselben DN erwartet, der im Bereitstellungsverzeichnis gespeichert ist.

Dieses Beispiel funktionierte nicht:

```
eTORADirectoryName=WSDLOracle4,eTNamespaceName=Oracle Server,dc=im,dc=eta
```

Dieses Beispiel ist der DN, der funktioniert hat:

```
EndPoint=WSDLOracle4,Namespace=Oracle Server,Domain=im,Server=Server
```

Lösung:

Um die Zuordnung zu finden, müssen Sie sich vergewissern, dass die Protokollebenen des Anwendungsservers auf "verbose" festgelegt sind. Führen Sie die Identity Manager-Aufgaben aus, für die Sie die Daten/Pfade benötigen. Die Pfade werden in der Protokolldatei sein. Die Suche mit "<" und "Einfügung in IM_" kann hilfreich dafür sein, die Pfade und auch die Attributwerte zu finden, die von den Aufgaben übergeben werden.

Fehler mit "setpasswd" bei 64-Bit-Linux-Systemen

Symptom:

Auf Linux 64-Bit- und Solaris-Systemen führt "setpasswd" zu folgendem Fehler: `"/opt/CA/SharedComponents/csutils/bin/expect: error while loading shared libraries: libtcl8.4.so: cannot open shared object file: No such file or directory"`

Lösung:

Legen Sie für LD_LIBRARY_PATH folgenden Wert fest:

/opt/CA/SharedComponents/csutils/lib/tcl8.4

Danach generiert "setpasswd" nicht mehr diesen Fehler.

Problem mit Kennwortrichtlinien bei Verwendung eines kombinierten Benutzerspeicher- und Bereitstellungsverzeichnisses

Symptom:

CA Identity Manager wendet bestimmte Kennwortrichtlinien nicht bei Bereitstellungen an, die ein kombiniertes Benutzerspeicher- und Bereitstellungsverzeichnis verwenden. Dieses Problem tritt mit Kennwortrichtlinien auf, die die folgenden Regeln und Einschränkungen enthalten:

- Ablauf des Kennworts:
  - Fehlgeschlagene oder erfolgreiche Anmeldeversuche verfolgen
  - Anmeldung authentifizieren
  - Das Kennwort läuft ab, wenn es nicht geändert wird
  - Kennwort-Inaktivität
  - Ungültiges Kennwort
  - Mehrere reguläre Ausdrücke
- Beschränkungen für Kennwort:
  - Mindestanzahl von Tagen vor Wiederverwendung
  - Mindestanzahl von Kennwörtern vor Wiederverwendung
  - Prozentualer Unterschied zum letzten Kennwort
  - Bei der Prüfung auf Unterschiede Sequenz ignorieren

Dieses Problem tritt auf, weil %PASSWORD_DATA% standardmäßig einem binären Attribut anstelle eines Zeichenfolgenattributs zugeordnet wird.

Lösung:

Ordnen Sie in der Management-Konsole %PASSWORD_DATA% einem "eTCustomField"-Attribut zu, das keinem anderen Attribut zugeordnet ist. Zum Beispiel eTCustomField99.

Nachdem Sie die Zuordnung aktualisiert haben, starten Sie die Umgebung neu.

Hinweis: Weitere Informationen zum Aktualisieren eines vorhandenen CA Identity Manager-Verzeichnisses finden Sie im *Konfigurationshandbuch*.

Verbindung zum CA IdentityMinder-Server kann nicht hergestellt werden, wenn der Kennwortsynchronisierungs-Agent für 64-Bit-Active Directory konfiguriert wird

Symptom:

Wenn der 64-Bit-Kennwortsynchronisierungs-Agent konfiguriert ist, kann ich keine Verbindung zum CA Identity Manager-Server herstellen, um die Liste der verfügbaren Active Directory-Endpunkte abzurufen.

Lösung:

Sie können nur die Chiffren konfigurieren, die CA IAM CS verwendet. Fügen Sie die drei neuen SSL-FIPS-Chiffren der Chiffrensammlung hinzu, die CA IAM CS verwendet.

Gehen Sie wie folgt vor:

1. Öffnen Sie die folgende Konfigurationsdatei in einem Texteditor:

   ```
   cs_home\jcs\conf\server_osgi_shared.xml
   ```

2. Suchen Sie die Eigenschaft "defaultCipherSuite" in der Datei. Der folgende Beispielcode in der Datei:

   ```
   <property
   name="defaultCipherSuite"><value>FIPS_TLS_PLUS_SSL_Ciphers</value></property>
   <property name="cipherSuites">
               <map>
                   <entry key="FIPS_TLS_PLUS_SSL_Ciphers">
                       <list>
                           <value>TLS_RSA_WITH_AES_128_CBC_SHA</value>
                           <value>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</value>
                           <value>TLS_DHE_DSS_WITH_AES_128_CBC_SHA</value>
                         </list>
   ```

   In diesem Beispiel ist *FIPS_TLS_PLUS_SSL_Ciphers* die Standard-Suite, die der Liste von Chiffren unter der Eigenschaft "cipherSuites" entspricht.

3. Fügen Sie folgende Eingaben der Liste hinzu:

   ```
   <value>SSL_RSA_WITH_3DES_EDE_CBC_SHA</value>
   <value>SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA</value>
   <value>SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA</value>
   ```

4. Klicken Sie auf "Speichern".

5. Starten Sie den CA IAM CS-Dienst neu.

   Der Kennwortsynchronisierungs-Agent für 64-Bit-Active Directory kann nun ohne Fehler verbunden werden.

Workflow-Teilnehmer-Resolver schlägt für EnableUserEventRoles fehl

Symptom:

Wenn Sie versuchen, Workflow-Einstellungen für die Aufgabe zu ändern, wird folgende Meldung angezeigt:

```
Die Option "Primäres Objekt dieser Aufgabe" kann nicht im Abschnitt {0}
'Auflösung - Beschreibung' für die Mehrfachauswahl-Aufgaben festgelegt werden.
```

Lösung:

Gehen Sie zur Workflowseite, und ändern Sie den Genehmiger in "Diesem Ereignis zugeordnetes Objekt".

Doppelter Name in "Gesendete Aufgaben anzeigen"

Symptom:

In einigen Hochverfügbarkeitsumgebungen mit hohen Lasten kann der CA Identity Manager-Server dem Bereitstellungsserver gleichzeitige Anfragen senden und Wettlaufsituationen im Bereitstellungsserver einführen, wenn parallele Änderungsanforderungen an denselben globalen Benutzer verarbeitet werden.

Lösung:

Ändern Sie die folgende Bereitstellungsmanager-Einstellung in "Nein", und starten Sie den Bereitstellungsserver neu.

```
Identity Manager-Server/Gleichzeitige Änderung am gleichen globalen Benutzer
zulassen
```

Hinweis: Wenn es eine Option zum Beenden des Programms beim Zugriff auf globale Benutzer gibt, lassen Sie diese Parametereinstellung auf "Ja".

Fehlermeldung "Nicht gefunden" beim Erstellen einer neuen Umgebung in manchen Bereitstellungen

Wenn CA Identity Manager mit CA SiteMinder 6.0.5 CR 31 oder späteren Versionen integriert wird, wird möglicherweise die Fehlermeldung "Fehler 404 - Nicht gefunden" angezeigt, wenn Benutzer versuchen, nach einer neuen Umgebungs-URL zu suchen.

Dieses Problem besteht aufgrund eines Zwischenspeicher-Problems im Richtlinienserver.

Behelfslösung

Gehen Sie folgendermaßen vor, um dieses Problem zu beheben:

Windows:

1. Geben Sie wie folgt ein Kennwort in die SiteMinder-Registrierung ein:
   a. Navigieren Sie zu \\HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\Siteminder\CurrentVersion\ObjectStore
   b. Fügen Sie den "ServerCmdMsec"-Schlüssel mit folgenden Einstellungen hinzu:
      - Typ: "DWORD"
      - Wert: 1
   c. Starten Sie den Richtlinienserver neu
2. Starten Sie den Anwendungsserver neu.
3. Schließen Sie alle Browser-Instanzen. Verwenden Sie dann eine neue Browser-Instanz, um auf die Umgebungs-URL zuzugreifen.

Solaris:

1. Fügen Sie eine Zeile hinzu zu <CA_HOME folder>/netegrity/siteminder/registry/sm.registry file ServerCmdMsec= 0x1 REG_DWORD
2. Starten Sie den Richtlinienserver neu.
3. Starten Sie den Anwendungsserver neu.
4. Schließen Sie alle Browser-Instanzen. Verwenden Sie dann eine neue Browser-Instanz, um auf die Umgebungs-URL zuzugreifen.

Ändern von zusammengesetzten Attributen mit einzelnem Wert im Identity Manager

Wenn Sie ein zusammengesetztes Attribut mit einzelnem Wert in CA Identity Manager für einen dynamischen Endpunkt ändern, legen Sie nur einen einzelnen Wert fest. Wenn Sie mehrere Werte festlegen, wird der bestehende Wert gelöscht und das Attribut verfügt über keinen Wert. Dieses Problem tritt im Bereitstellungs-Manager nicht auf.

Beschränkungen des Massendatenladers auf Beziehungsattribut-Ebene

Der Massendatenlader kann die Aufgabenvorgänge auf den Benutzerobjekten nicht auf der Beziehungsattributebene aktualisieren.

- Beziehungsattribute, die nicht vom Massendatenlader aktualisiert werden, sind Benutzerzugriffsrollen, Benutzer-Admin-Rollen, Benutzer-Bereitstellungsrollen, Benutzergruppenmitgliedschaft und Gruppen.
- Beziehungsattribute, die überschrieben werden würden, wenn Sie alte Attributwerte durch neue Attributwerte aus der Massendatenladerdatei ersetzen, sind Gruppen-Administratoren und benutzerdefinierte oder Standard-Attribute mit mehreren Werten.

Fehler beim Erstellen einer bereitstellungsaktivierten Umgebung mithilfe von Token-Vorlagen

In diesem Fall kann CA Identity Manager die Rolle des Bereitstellungs-Synchronisations-Managers nicht dem im Umgebungserstellungsassistenten definierten eingehenden Administrator zuweisen.

Wenn die Umgebungsvorlage Token oder übersetzte Zeichenfolgen für den Rollennamen des Bereitstellungs-Synchronisations-Managers hat, schlägt die Suche fehl und der NoSuchObjectException-Fehler wird ausgelöst.

Voraussetzungen für Oracle-Anwendungen

Sie müssen NLS_LANG als eine Systemumgebungsvariable mit dem Wert .UTF8 festlegen.

Hinweis: Der Punkt (.) muss vor UTF8 auf dem System stehen, wo der Connector-Server installiert wird.

Oracle 11gR2 RAC-Benutzerspeicher: Groß- und Kleinschreibung bei der Suche

Symptom:

Wenn Oracle 11gR2 RAC der Benutzerspeicher ist, ergibt die Suche nach Benutzern, Gruppen oder Organisationen manchmal bietet keine Ergebnisse, obwohl die Objekte vorhanden sind.

Lösung:

Für diesen Benutzerspeicher muss bei der Suche die Groß-/Kleinschreibung beachtet werden. Zum Beispiel liefert die Suche nach *Schmidt* keine Ergebnisse, wenn der Benutzer als *SCHMIDT* in der Datenbank erstellt wurde. Verwenden Sie die gleiche Schreibweise, mit der das Objekt in der Datenbank erstellt wurde.

CA Identity Manager unter JBoss nimmt Verbindung zu Oracle nicht wieder auf

Symptom:

Bei Verwendung von JBoss 5.x mit der Datenquelle einer Oracle-Datenbank und beim Upgraden von CA Identity Manager auf Version r12.5 fällt beim Neustart des Datenbankservers die Anwendung aus. Der Ausfall wird verursacht, weil JBoss die Eigenschaft "background-validation-minutes" durch "background-validation-millis" ersetzt.

Lösung:

Gehen Sie folgendermaßen vor, um dieses Problem zu beheben:

1. Halten Sie den Anwendungsserver an.
2. Öffnen Sie die Datenquellendateien unter */JBoss-Ordner/Server/Standard [oder Servername in Cluster]/deploy* , und löschen Sie die folgende Zeile:

   <background-validation-minutes> </background-validation-minutes>
3. Fügen Sie folgende Zeile hinzu:

   <background-validation-millis>120000</background-validation-millis>

   Hinweis: 120000 ist das Äquivalent zu 2 Minuten, die früher standardmäßig für "background-validation-minutes" angegeben wurden. Konfigurieren Sie den Wert entsprechend den Geschäftsanforderungen.
4. Starten Sie den Anwendungsserver neu.

Hinweis: Das Problem hat keine Auswirkungen auf die neue Installation von CA Identity Manager.

Fehler bei "Zum Hauptinhalt wechseln" in Mozilla Firefox

Symptom:

Oben in der Benutzerkonsole sehen Sie den Link "Zum Hauptinhalt wechseln". Dieser Link verschiebt den Hauptrahmen der Seite an das obere Ende. Allerdings schlägt dieser Link in Mozilla Firefox fehl.

Lösung:

Verwenden Sie Microsoft Internet Explorer 8 oder höher mit JAWS, um diese Funktion zu unterstützen.

Fehler bei gleichzeitigen Änderungen an einem Benutzer

Die Aufgabe "Benutzer ändern" schlägt in folgenden Situationen fehl:

- Wenn Sie versuchen, einen Benutzer zu deaktivieren, während Sie diesen Benutzer ändern, schlägt die Aufgabe fehl.
- Wenn Sie das Attribut "forcePasswordChange" dem Fenster "Benutzerprofil" hinzufügen, während Sie einen Benutzer ändern, schlägt die Aufgabe fehl.

Änderung an Policy Xpress-Syntax

Symptom:

Aufgrund einer Änderung an der Policy Xpress-Syntax kann ein Fehler auftreten. Der Fehler tritt auf, wenn die Richtlinie die Zeichenfolgenanalyse für die Konto-ID verwendet und der Benutzer mehrere Konten auf einem flachen Endpunkt hat. Endpunkte wie Oracle, OS400 und Microsoft SQL haben Konten als virtuelle Container, die sich unter dem Endpunktnamen befinden. Beim Starten unter 12.6.1 ist die Syntax der Konto-ID folgendermaßen:

- Für flache Connectors, EndpointName: EndpointName:AccountName
- Für hierarchische Connectors, EndpointName:AccountContainerPath:AccountName

Lösung:

Suchen Sie die Policy Xpress-Richtlinien, die die Zeichenfolgenanalyse für die Konto-ID verwenden. Aktualisieren Sie diese Richtlinien entsprechend der neuen Syntax.

Aktualisieren gemäß SAP-Hilfethema

Die Hilfe für die auf SAP r3-Konten bezogene Standardsregisterkarte sollte diese Definition für die Dezimale Notation haben.

- Gibt die unterschiedlichen Dezimalschreibweisen an.
- Folgende Optionen stehen zur Auswahl:

  1.234.567,89

  1,234,567.89

  1 234567,89

Aktivieren Sie den Fix für Oracle-Fehler 6376915

Der Oracle-Fehler 6376915 verursacht Enqueue-Konflikte bei "High Water" (HW), wenn die Datenbank mit der Verarbeitung großer Objekte (LOB) beschäftigt ist, und wenn die Datenbank zur Verwendung von ASSM (automatic segments space management) konfiguriert ist.

Dieser Fehler verursacht Leistungs- und Skalierbarkeitsprobleme mit der CA-Software, einschließlich CA Identity Manager und CA CloudMinder.

Der Fix für dieses Problem führt ein obligatorisches Ereignis ein. Legen Sie dieses neue Ereignis fest, um die ASSM-Architektur effizienter an LOB-Datenblöcke zuzuordnen.

Dieser Fehler wurde in Oracle 10.2.0.3 eingeführt. Der Fehler wurde sowohl in Oracle 10.2.0.4 als auch in Oracle 11.1.0.7 behoben. Allerdings ist der Fix nicht standardmäßig aktiviert.

Für die Schritte in diesem Vorgang wird angenommen, dass "spfile" für die Konfiguration verwendet wird.

Gehen Sie wie folgt vor:

1. Geben Sie folgenden Befehl ein:

   ```
   ALTER SYSTEM SET EVENT='44951 TRACE NAME CONTEXT FOREVER, LEVEL
   1024' scope=spfile;
   ```

2. Starten Sie die Datenbank erneut.
3. Um den Fix zu testen, gehen Sie folgendermaßen vor:
   - Verwenden Sie den Massendatenlader, um den Aufgabendurchsatz in CA Identity Manager und CA CloudMinder zu messen.
   - Messen Sie die Wartezeit für HW-Enqueue-Konflikte.

Fehler beim Ausführen der Aufgabe "RequestUserToService"

Symptom:

Wenn Oracle 12c als Objektspeicher mit JBoss 6.x als Anwendungsserver verwendet wird, wird eine Fehlermeldung zum Fehlschlag von RequestUserToService zurückgegeben. FEHLERMELDUNG: SmApiWrappedExceptionRA-01843: not a valid month" is displayed in the UI when a user is requesting for a Service.

Lösung:

1. Halten Sie den JBoss 6.x-Anwendungsserver an.
2. Bearbeiten Sie die Datei **Standalone-full.xml**. Sie befindet sich unter **<JBoss-Installationsverzeichnis>\Standalone\Configuration**.
3. Suchen Sie nach folgendem Text:
   `jndi-name="java:/iam/im/jdbc/jdbc/objectstore".`
4. Fügen Sie die hervorgehobene Zeile hinzu:
   ```
   <datasource jta="false" jndi-
   name="java:/iam/im/jdbc/jdbc/objectstore" pool-name="iam_im-
   imobjectstoredb-ds" enabled="true" use-java-context="true">
   <connection-
   url>jdbc:sqlserver://<hostname>:1433;selectMethod=cursor;Databa
   seName=<ora_dbname></connection-url>
   <driver>sqljdbc</driver>

   <new-connection-sql>alter session set NLS_DATE_FORMAT='YYYY-MM-
   DD' NLS_TIMESTAMP_FORMAT='YYYY-MM-DD HH24:MI:SS.FF3'</new-
   connection-sql>
   ```
5. Fügen Sie die unten angezeigte hervorgehobene Zeile zur Datei hinzu, und speichern Sie die Datei.
   ```
   <datasource jta="false" jndi-
   name="java:/iam/im/jdbc/jdbc/reportsnapshot" pool-name="iam_im-
   imreportsnapshotdb-ds" enabled="true" use-java-context="true">
   <connection-
   url>jdbc:sqlserver://<hostname>:1433;selectMethod=cursor;Databa
   seName=<ora_dbname></connection-url>
   <driver>sqljdbc</driver>

   <new-connection-sql>alter session set NLS_DATE_FORMAT='YYYY-MM-
   DD' NLS_TIMESTAMP_FORMAT='YYYY-MM-DD HH24:MI:SS.FF3'</new-
   connection-sql>
   ```
6. Starten Sie den Anwendungsserver.

Berichterstellung

Folgende Probleme hängen in CA Identity Manager r12.5 SP1 mit der Berichterstellung zusammen.

Audit - Bericht über zugewiesene oder entfernte Bereitstellungsrollen

Symptom:

"Audit - Bericht über zugewiesene oder entfernte Bereitstellungsrollen" wird ohne Daten generiert, wenn Windows AD 2012 R2 als Benutzerspeicher verwendet wird.

Lösung:

1. Melden Sie sich bei der IdentityMinder-Management-Konsole an.
2. Klicken Sie auf den Link "Umgebungen" und anschließend auf Ihre <AD-Umgebung>.
3. Klicken Sie auf "Erweiterte Einstellungen", "Überprüfung".
4. Klicken Sie auf die Schaltfläche "Exportieren".
5. Speichern Sie die XML-Datei mit den Audit-Einstellungen.
6. Öffnen Sie die XML-Datei mit den Audit-Einstellungen, und fügen Sie am Ende der Datei die folgenden Zeilen hinzu:
```
<AuditEvent name="RevokeProvisioningRoleEvent" enabled="true"
auditlevel="BOTHCHANGED">
    <AuditProfile objecttype="USER" auditlevel="BOTHCHANGED"/>
    <EventState name="COMPLETE" severity="NONE"/>
    <EventState name="INVALID" severity="CRITICAL"/>
 </AuditEvent>
```
7. Speichern Sie die Datei.
8. Wiederholen Sie die Schritte 1, 2 und 3.
9. Klicken Sie auf die Schaltfläche "Importieren", durchsuchen Sie das System nach der aktualisierten XML-Datei mit den Audit-Einstellungen, wählen Sie sie aus, und klicken Sie auf "Fertig stellen".
10. Starten Sie die Umgebung neu.
11. Generieren Sie den Bericht, um "Audit - Bericht über zugewiesene oder entfernte Bereitstellungsrollen" mit Daten zu erstellen.

Bei der Benutzerfiltersuche ist in den Benutzerkonten und den XML-Dateien zu benutzerdefinierten Snapshots der Endpunktkonten die Groß-/Kleinschreibung zu beachten.

Symptom:

Beim Erstellen eines Filters auf %USER_ID% in den *useraccounts*-Exportelementen in *Benutzerkonten* und den XML-Dateien zu benutzerdefinierten Snapshots der *Endpunktkonten* zeigt der Bericht die Ergebnisse nicht an, obwohl der Benutzer vorhanden ist.

Lösung:

Bei der Filtersuche muss die Groß-/Kleinschreibung beachtet werden.

Satisfy=All funktioniert in XML-Datei nicht ordnungsgemäß

In einer XML-Datei mit Snapshot-Parametern reagieren die Parameter satisfy=all und satisfy=any beide identisch mit satisfy=any (ähnlich wie ein OR-Operator).

Problem beim Verwenden mehrerer Filter auf Endpunktobjekten

Symptom:

Wenn eine Snapshot-Definition mit Endpunktobjekt mithilfe mehrerer Filter erstellt wird, werden keine Endpunktdaten erfasst.

Lösung:

Auf der Registerkarte "Snapshotrichtlinien" wird anstelle der Auswahl mehrerer Endpunktobjekte das "*"-Sternchen angeben, um mehrere Endpunktobjekte auszuwählen.

Snapshot erfasst keine Gruppenobjektdaten

Symptom:

Wenn eine Snapshot-Definition mit einem Gruppenobjekt und unter Verwendung von "org-filter" erstellt wird, werden keine Gruppendaten erfasst.

Lösung:

Auf der Registerkarte "Snapshotrichtlinien" wird im Drow-down-Menü anstelle der Auswahl von "org-filter" die Option "(alle)" ausgewählt.

Allgemein

Folgende sind allgemeine Bereitstellungsprobleme in CA Identity Manager r12.5 SP1.

Umbenennen von Bereitstellungsrollen wird nicht unterstützt

Das Umbenennen von Bereitstellungsrollen, nachdem sie erstellt wurden, wird nicht unterstützt.

Solaris ECS-Protokollierung oberhalb der INFO-Ebene kann die Leistung des Bereitstellungsservers verringern

Das Aktivieren der ECS-Protokollierung oberhalb der INFO-Ebene führt dazu, dass Protokolle geschrieben werden, bevor Sie eine Antwort erhalten. Dadurch wird Ihre Anfrage verzögert, während das Protokoll geschrieben wird.

Behelfslösung

Deaktivieren Sie die ECS-Protokollierung, falls Sie feststellen, dass die Leistung des Bereitstellungsservers beeinträchtigt ist.

Fehler "Bereits vorhanden" beim Hinzufügen eines Endpunkts

Wenn Sie einen Endpunkt löschen und mit genau demselben Namen wieder hinzufügen, gibt der Bereitstellungsserver manchmal eine Fehlermeldung aus, dass bereits ein Endpunkt mit dem Namen existiert. Dies kann auftreten, wenn Sie mehrere Connector-Server zum Verwalten des Endpunkts konfiguriert haben. Der Grund für das Fehlschlagen ist ein Problem beim Löschen des Endpunkts, bei dem nicht alle Connector-Server vom Löschen benachrichtigt wurden.

Behelfslösung

Starten Sie alle Connector-Server, die für die Endpunktverwaltung konfiguriert sind, neu.

Fehler bei der Korrelation eines Microsoft SQL-Endpunkts

Symptom:

Die Korrelation eines Microsoft SQL-Endpunkts schlägt mit der folgenden Meldung fehl:
`Object MS SQL Logins global users creation failed. Unable to determine object class from distinguished name.`

Dieser Fehler tritt auf, wenn für einen Microsoft SQL-Endpunkt alle Container und nicht nur die Container mit Konten ausgewählt werden.

Lösung:

1. Erstellen Sie eine Definition für "Durchsuchen und Korrelieren", und suchen Sie nach einem Microsoft SQL-Endpunkt.
2. Suchen Sie nach allen Containern, aber wählen Sie nur den *Endpunktnamen* als Container aus.
3. Wählen Sie "Durchsuchen und Korrelieren"-Attribute aus.
4. Führen Sie die Definition "Durchsuchen und Korrelieren" aus.

Einschränkung beim SiteMinder-Anmeldenamen für globalen Benutzernamen

Folgende Zeichen oder Zeichenfolgen darf ein globaler Benutzername nicht enthalten, wenn der Benutzer sich auf dem SiteMinder-Richtlinienserver anmelden können soll:

```
&
*
:
()
```

Behelfslösung

Vermeiden Sie die Verwendung dieser Zeichen im globalen Benutzernamen.

CA IAM CS und Connector Xpress

Die folgenden Probleme beziehen sich auf CA IAM Connector Server (CA IAM CS) und Connector Xpress.

Hinweis: In CA Identity Manager 12.6 ist Java Connector Server (Java CS oder JCS) in CA IAM Connector Server umbenannt worden (CA IAM CS).

JNDI-Kontoverwaltungsfenster – das Erstellen von Konten mit mehreren strukturierten Objektklassen schlägt fehl

Sie können keine Konten mit mehreren strukturierten Objektklassen erstellen.

Endpunkttypen

Folgende Probleme hängen in CA Identity Manager r12.5 SP1 mit der Verwaltung von Endpunkttypen zusammen.

Allgemein

Die folgenden Abschnitte beschreiben die für die verschiedenen Connectors bekannten Probleme:

Kontostatus von nicht vorhandenen Konten wird in der CA Identity Manager-Benutzerkonsole nicht richtig angezeigt

In der CA Identity Manager-Benutzerkonsole wird der Kontostatus von einem systemeigenen gelöschten Konto nicht richtig angezeigt. Eine Erfolgsmeldung wird angezeigt, wenn Sie einen Endpunkt deaktivieren, der nicht vorhanden ist.

Endpunkte mit automatischer Wiederholungsversuchssperre müssen mit einem großzügigen Limit für Wiederholungsversuche konfiguriert werden.

Dieser Abschnitt bezieht sich auf alle TSS-Connectors.

Beachten Sie einen Endpunkt, deren Sperrwert für automatische Wiederholungsversuche bei "N" liegt. Das Konto, das zur Verbindung mit dem Endpunkt verwendet wird, der CA IAM CS verwendet, so konfiguriert sein, dass es einen großzügigen (oder unbegrenzten) Wert "N" besitzt, da die Zahl der Verbindungsversuche vom CA IAM CS schnell erreicht ist.

Wenn das Konto vom System gesperrt wird, weil der "N"-Wert überschritten wurde, kann die Verwendung systemeigener Tools zur Entsperrung des Kontos erforderlich sein, um wieder auf den Endpunkt zugreifen zu können. Diese Situation hängt vom exakten systemeigenen Sperrverhalten des Endpunkts ab.

Fehler in Endpunkt-Suchfenstern nach dem Upgrade von CA Identity Manager r12.5 SP6 oder älter

Dieser Abschnitt bezieht sich auf alle TSS-Connectors.

Symptom:

Ein Fehler, der der folgenden Meldung ähnelt, tritt auf, wenn Sie Rollendefinitionsdateien von Endpunkt aus r12.5 SP6 oder älter in r12.5 SP7 oder höher importieren:

"Error in screen definition "Default Endpoint Type Primary Group Endpoint Capability Search" with tag "DefaultActiveDirectoryPrimaryGroupEndpointCapabilitySearch" Error: The type "UNKNOWN" is not a valid object type."

In CA Identity Manager r12.5 SP7 wurden bestimmte Objekte umbenannt. Auf diese Objekte wird in Endpunktfunktions-Suchfenstern verwiesen. Nach dem Upgrade auf r12.5 SP 7 oder höher kann ein Fehler auftreten, wenn Sie Rollendefinitionsdateien importieren, die Fenster einschließen, die sich auf die alten Objektnamen beziehen.

Dieses Problem ist in Active Directory und CA Access Control-Endpunkten identifiziert worden.

Lösung:

Löschen Sie ggf. die Bildschirmdefinitionen, die sich auf den alten Objektnamen beziehen, bevor Sie eine Rollendefinitionsdatei importieren.

Folgender Fall ist ein Beispiel für einen Active Directory-Endpunkt:

In CA Identity Manager r12.5 SP6 bezog sich der Suchfenstername von Active Directory-Endpunkten auf das Objekt ACTIVEDIRECTORY_ADUNIXPRIMARYGROUP.

Der Objektname wird in der folgenden Bildschirmdefinition angezeigt:

```
<Screen name="Default Active Directory Primary Group Endpoint
Capability Search"
tag="DefaultActiveDirectoryPrimaryGroupEndpointCapabilitySearch"

screendefinition="EndpointCapabilitySearch"

Object="ACTIVEDIRECTORY_ADUNIXPRIMARYGROUP">
```

In CA Identity Manager r12.5 SP7 wurde der Objektname in "ACTIVEDIRECTORY_ETADSGROUP" geändert.

Der neue Objektname wird in der folgenden Bildschirmdefinition angezeigt:

```
<Screen name="Default Active Directory Group Endpoint Capability Search"

tag="DefaultActiveDirectoryGroupEndpointCapabilitySearch"

screendefinition="EndpointCapabilitySearch"

object="ACTIVEDIRECTORY_ETADSGROUP">
```

Kontovorlagen sind in der Benutzerkonsole auf einem "Erstellen"- oder "Verändern"-Task nicht mit Konten synchronisiert.

Symptom:

Die Benutzerkonsole unterstützt keine explizite Kontensynchronisierung.

Lösung:

Verwenden Sie den Bereitstellungs-Manager, um Konten mit Kontovorlagen zu synchronisieren.

Einen Endpunkt direkt zu verändern, verursacht einen Fehler beim Importieren zwischen Endpunkt und Bereitstellungsserver.

Dieser Abschnitt bezieht sich auf alle TSS-Connectors.

Wenn der Endpunkt direkt geändert wird (nicht mithilfe des Bereitstellungsservers), wird beim Importvorgang ein Fehler zurückgegeben. Dieser Fehler tritt auf, da inkonsistente Daten zwischen dem Endpunkt und dem Bereitstellungsserver vorhanden sind. Zwei Beispiele:

- Es wurden unter Verwendung von systemeigenen Tools Tabellen vom MSSQL-Endpunkt entfernt, was dazu führte, dass manche Benutzer nicht mehr vorhandene Ressourcen erhielten.

  Um den Fehler zu beheben, durchsuchen Sie den Endpunkt mit Hilfe des Bereitstellungsservers erneut.

- Jemand hat einige Serverrollen auf dem Endpunkt gelöscht. Die Kontovorlagen, die diese zugewiesenen Serverrollen immer noch zugeordnet hatten, haben zusätzliche Rollen erhalten, die nicht mehr auf dem Endpunkt vorhanden sind.

  Um den Fehler zu beheben, entfernen Sie diese "beseitigten" Serverrollen manuell von den Kontovorlagen.

Einschränkung für den Endpunktnamen von ACF2 ACFESAGE-, RACF IRRDBU00- und TSSCFILE-Connectors

Symptom:

Wenn Sie versuchen, einen Endpunkt mit einem Endpunktnamen wie "Benutzer testen", "Benutzer-Test" oder "_Benutzertest" auf Dumpfile-Connectors zu erstellen, wird bei der Endpunkterstellung ein Fehler mit folgender Meldung verursacht: "Cannot create pool able connection factory" (Es konnte keine Pool-fähige Connection Factory erstellt werden).

Lösung:

Leerzeichen sind in Endpunktnamen für ACF2 ACFESAGE-, TSSCFILE- oder RACF-IRRDBU00-Connectors nicht mehr erlaubt. Der Endpunktname für diese Connectors hat auch die folgenden Einschränkungen:

- Muss zwischen 1 und 30 Zeichen lang sein
- Fängt mit alphanumerischen Zeichen an
- Enthält nur alphanumerische Zeichen und/oder "_"-Zeichen.

Bevor Sie ein Upgrade auf diese Version durchführen, löschen Sie die vorhandenen Mainframe-Dumpfile-Endpunkte, deren Namen nicht den Einschränkungen entsprechen.

CA Access Control

Texte der Schaltflächen des Kalenderfensters sind in Englisch

Wenn Sie im CA Access Control-Endpunkt eine Kontovorlage erstellen, werden im Kalenderfenster unter der Registerkarte "Anmeldung" die Schaltflächen "OK" und "Abbrechen" auf Englisch angezeigt.

Entfernen von Gruppen aus einem Access Control-Konto

Symptom:

Wenn Sie eine systemeigene Gruppe aus einem systemeigenen Benutzerkonto entfernen, das vom Access Control Connector bereitgestellt wurde, werden die systemeigenen Gruppen in einem zweistufigen Prozess entfernt. Der zweistufige Prozess entfernt alle vorhandenen Gruppenmitgliedschaften und fügt dann alle erforderlichen Gruppenmitgliedschaften wieder hinzu. Dies sorgt für die korrekte Gruppenmitgliedschaft des Kontos, kann bei einigen Kunden aber zu betrieblichen Problemen führen.

Lösung:

Wenn Sie den zweistufigen Prozess nicht verwenden möchten, können Sie Connector XPress verwenden, um eine C++ Connector Server (CCE)-Definition zu erstellen. Die CCE-Definition kann direkt mit dem Bereitstellungsserver verbunden werden anstelle eines Routings über CA IAM CS. Diese Umgehungslösung führt zu einer einstufigen Gruppenänderung für ACC-Konten. Allerdings können Sie die Benutzerkonsole nicht verwenden, um ACC-Kontogruppenmitgliedschaften zu verwalten. Um ACC-Kontogruppenmitgliedschaften zu verwalten, verwenden Sie den Bereitstellungsmanager.

Hinweis: Weitere Informationen zur Verwendung von Connector Xpress für die Erstellung einer C++ Connector Server-Definition finden Sie unter "How You Set a Managing Connector Server" (Einrichten eines verwaltenden Connector-Servers) im *Connector Xpress-Handbuch*.

CA Arcot

Schützen von ArcotID-Aufgaben, wenn SiteMinder CA Identity Manager schützt

Wenn SiteMinder CA Identity Manager mithilfe eines CA AuthMinder-Authentifizierungsschemas schützt, werden folgende Aufgaben in CA Identity Manager deaktiviert:

- Meine ArcotID erstellen/zurücksetzen
- Meine ArcotID herunterladen

Der Grund dafür ist, dass SiteMinder ein Authentifizierungsschema für eine geschützte Ressource definiert. Alle CA Identity Manager-geschützten Aufgaben haben die gleiche URL, die von einem SiteMinder-Authentifizierungsschema geschützt wird. Dadurch deckt das gleiche Authentifizierungsschema alle CA Identity Manager-Aufgaben ab.

Wenn die ArcotID-Authentifizierung die CA Identity Manager-URL schützt, müssen Benutzer eine ArcotID angeben, um auf Aufgaben zuzugreifen. Benutzer, die auf die oben aufgelisteten Aufgaben zugreifen, haben noch keine ArcotID. Sie können diese also nicht bereitstellen, um auf die Aufgaben zugreifen zu können.

Um dieses Problem zu verhindern, verwenden Sie ein Authentifizierungsschema außer CA AuthMinder, wenn SiteMinder CA Identity Manager-Aufgaben schützt. Beispiele: Active Directory oder LDAP.

Hinweis: "Meine ArcotID erstellen / zurücksetzen" oder "Meine ArcotID herunterladen" sind sensible Aufgaben. CA Technologies empfiehlt dringend, dass Sie diese Aufgaben als geschützte Aufgaben konfigurieren. Wenn Sie diese Aufgaben als öffentliche Aufgaben konfigurieren, können Benutzer auf diese zugreifen, ohne Anmeldeinformationen anzugeben. Weitere Informationen zu öffentlichen Aufgaben finden Sie unter Self-Service-Aufgaben im "Benutzerkonsolendesign-Handbuch".

CA SSO für den Connector des Servers für erweiterte Richtlinien

Folgende Abschnitte beschreiben die bekannten Probleme für den CA SSO Connector des Servers für erweiterte Richtlinien:

PLS-Connector kann nicht mehr als 2000 Konten zu Anwendungen hinzufügen

Es können nicht mehr als 2000 PLS-Konten gleichzeitig zu einer Anwendung hinzugefügt werden. Wenn Sie mehr als 2000 PLS-Konten hinzufügen möchten, müssen Sie die Konten in mehrere Operationen aufteilen.

DB2 und DB2 für z/OS

Folgende Abschnitte beschreiben die bekannten Probleme für die DB2 und DB2 für z/OS Connectors:

Fehler beim Speichern eines Datum-Datentyps aufgrund eines Datentypenkonflikts

Symptom:

Wenn ich das Datumstypattribut auf einem DB2-Endpunkt (JDBC DB2 für IBM i) festlege, wird der folgende Fehler angezeigt:

```
Bad SQL Grammar: Data type mismatch. (YYYY-MM-DD)
```

Lösung:

Bearbeiten Sie die ConnectionURI auf der Endpunktseite des Bereitstellungsmanagers, und fügen Sie *date format=iso* hinzu. Die letzte URI wird wie folgt angezeigt:*jdbc:as400://<host>:CA Portal/<db>;prompt=false;date format=iso;*. Beachten Sie den Abstand zwischen *date* und *format*.

Google Apps

In den folgenden Abschnitten werden die bekannten Probleme für den Google Apps-Connector beschrieben:

Google-Apps: Fehlermeldung beim Erstellen von Google Apps-Konten

Symptom:

Beim Erstellen eines Google Apps-Kontos erhalte ich die Fehlermeldung *Ausführung von 'Google Apps-Benutzer erstellen' fehlgeschlagen. Google Apps-Benutzer wurde erstellt, jedoch schlug ein zusätzlicher Vorgang fehl*.

Das Konto wird in CA Identity Manager und auf dem Google Apps-Endpunkt erstellt, aber es ist in der CA CA Identity Manager-Benutzerkonsole nicht sichtbar, weil es nicht dem globalen Benutzer zugeordnet ist.

Lösung:

Der Fehler tritt auf, wenn Sie versuchen, ein Konto mit dem gleichen Spitznamen und Benutzernamen zu erstellen.

Um das Problem zu beheben, durchsuchen und korrelieren Sie den Google Apps-Endpunkt

Das Benutzerkonto, das Sie erstellt haben, ist dem globalen Benutzer in CA Identity Manager zugeordnet und wird nun angezeigt.

Google Apps - Mehrere Google Apps-Endpunkte auf demselben Java CS

Proxy-Einstellungen des Google Apps-Connectors sind systemübergreifende Eigenschaften. Wenn Sie zwei oder mehr Google Apps-Endpunkte auf dem gleichen Java CS erstellen, verwenden Sie den gleichen Proxy-Server, Port, Benutzernamen und Kennwort für alle Google Apps-Endpunkte auf demselben Java CS.

Google Apps - Fehlermeldung "HTTP 403: Verboten" bei Verwendung der NTLM-Authentifizierung

Symptom:

Wenn ich versuche, NTLM-Authentifizierung zu verwenden, erhalte ich den Fehler *HTTP 403: Verboten* vom Proxy-Server, und die Google Apps-Domäne wird nicht aufgerufen.

Lösung:

Der Fehler tritt auf, weil Java CS auf einem Windows-Computer als ein Windows-Dienst installiert wird und standardmäßig als lokales System ausgeführt wird.

Wenn Java CS auf einem Windows-Computer ausgeführt wird und NTLM das stärkste vom HTTP-Proxy unterstützte Authentifizierungsschema ist, versucht der Google Apps-Connector, NTLM-Authentifizierung mit dem HTTP-Proxy zu verwenden.

Wenn Ihr HTTP-Proxy-Server NTLM-Authentifizierung verwendet, konfigurieren Sie Java CS zur Ausführung unter einem Windows-Domänenkonto oder einem lokalen Windows-Konto.

So konfigurieren Sie die NTLM-Authentifizierung

Führen Sie einen der folgenden Schritte aus:

- Führen Sie Java CS mit einem Windows-Konto aus, das mit dem HTTP-Proxy-Server authentifiziert werden kann, ohne einen Benutzernamen und ein Kennwort für Proxyauthentifizierung anzugeben, wenn Sie den Endpunkt erstellen.
- Führen Sie Java CS mit einem Windows-Konto aus, das nicht mit dem HTTP-Proxy-Server authentifiziert werden kann, und geben Sie einen HTTP-Benutzernamen und ein Kennwort an, das mit dem Proxy authentifiziert werden kann, wenn Sie den Endpunkt erstellen.

Hinweis: Wenn Sie einen Windows-Domänenbenutzer für HTTP-Proxyauthentifizierung verwenden, setzen Sie die Windows-Domäne, in der sich der Benutzer befindet, als Präfix vor den HTTP-Proxy-Benutzernamen. Beispiel: "DOMAIN|ProxyBenutzerkontoname".

Kontosuchfehler von Google Apps

Symptom:

Die Suche nach einem Google Apps-Konto auf Basis des Vor- oder Nachnamens schlägt fehl.

Lösung:

Die Aktualisierung auf den Vor- oder Nachnamen eines Benutzers durch Google Apps kann bis zu 30 Minuten dauern. Deswegen schlägt die Suche nach dem neuen Namen in CA Identity Manager fehl. Warten Sie nach einer Namensänderung 30 Minuten, bevor Sie bei der Suche den neuen Namen verwenden.

Microsoft Active Directory und Exchange

Bekannte Probleme für Active Directory und Exchange sind jetzt im *Endpunkthandbuch für Active Directory und Exchange*. Sie können dieses Handbuch über CA Support herunterladen.

PeopleSoft

In den folgenden Abschnitten werden die bekannten Probleme für den PeopleSoft-Connector beschrieben:

Suchen können im Bereitstellungsmanager fehlschlagen

Wenn Sie den Bereitstellungsmanager verwenden, um nach einem PeopleSoft-Endpunkt mit PeopleTools 8.49 zu suchen, gibt die Suche nach PPS-Benutzern für die Zuweisung zu den Feldern "Alternative Benutzer-ID", "ID des überwachenden Benutzers" und "Arbeit neu zuweisen zu" in einigen Fällen keine Ergebnisse zurück.

Es gibt zwei Problemumgehungen für dieses Problem:

- Verwenden Sie die CA Identity Manager-Benutzerkonsole, um PeopleSoft-Endpunkte zu verwalten (bevorzugt).
- Geben Sie den Wert in die Bereitstellungsmanager-Felder ein, ohne Suchen auszuführen. Der Wert ist immer noch abhängig von der Validierung, sodass die Zuweisung beim Anklicken der Schaltfläche "Übernehmen" fehlschlägt, wenn der eingegebene Wert kein PPS-Benutzer ist.

SAP

Folgende Abschnitte beschreiben die bekannten Probleme für den SAP Connector:

SAP-vertragliche Benutzertypen zuweisen

Wenn ein vertraglicher Benutzertyp einem Benutzer auf der Registerkarte "Lizenzdaten" zugewiesen wird, kann die Änderung nur auf das Master-System und auf kein Tochter-System angewendet werden.

Behelfslösung

Die vertraglichen Lizenztypen für die untergeordneten Elemente können systemabhängig verändert werden.

Der SAP-Endpunkt wurde nicht vorher von der Datei "SAPlogon.ini " aufgefüllt.

Wenn der Bereitstellungs-Manager in Windows 2008 ausgeführt wird, werden die Endpunktdetails für SAP nicht vorher von der Datei "SAPlogon.ini" aufgefüllt.

Hinweis: Dieses Problem ist typisch für den nur auf Windows 2008 ausführbaren Bereitstellungs-Manager.

Behelfslösung

Sie müssen den Inhalt der Datei "SAPlogon.ini" manuell in den Bereitstellungs-Manager eingeben.

Pflichtfelder im SAP-Attribut "Vertraglicher Benutzertyp"

Der vertragliche Benutzertyp, der in der Registerkarte "Lizenzdaten" des Kontos angegeben ist, darf keine anderen Pflichtfelder enthalten als das Feld LIC_TYPE. Wenn Sie z. B. den Namen von einem SAP R3-System (SYSID) angeben sollen, um einen vertraglichen Benutzertyp zu verwenden, wird die Zuweisung fehlschlagen, und Sie erhalten eine Fehlermeldung, dass ein Wert für den Namen des SAP R3-Systems fehlt.

Das vertragliche Benutzertyp-Attribut in der Registerkarte für Kontolizenzdaten funktioniert nicht für alle Lizenztypen.

Wenn ein Benutzertyp aus der verfügbaren Liste ausgewählt wird, funktionieren nur manche Benutzertypen. Manche Lizenztypen verursachen den Funktionsaufruffehler 'BAPI'. Der Grund dafür ist, dass manche Benutzertypen Extrafelder enthalten, die nicht erkannt werden.

Siebel

Folgende Abschnitte beschreiben die bekannten Probleme für den Siebel Connector:

SBL-Fehler beim Erstellen eines Kontos an mehreren Endpunkten

Eine Kontovorlage, die mehrere Endpunkte auflistet, kann nur Siebel-Gruppen anzeigen, die auf allen Endpunkten bestehen.

UNIX v2

Das Zurücksetzen eines Benutzerkennworts funktioniert anders für verschiedene Plattformen

Wenn die Aufgabe "Benutzerkennwort zurücksetzen" in Suse- und HPUX-Endpunkten ausgeführt wird, wird das Benutzerkonto vom ausgesetzten Status aktiviert. Aber im Fall von RHEL-, Solaris- und AIX-Endpunkten bleibt das Benutzerkonto im ausgesetzten Status.